VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

NÁVRH ZABEZPEČENÍ HERNÍHO SERVERU
GAME SERVER SECURITY DESIGN

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — **Bc. Milan Marek**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. Petr Sedlák**
SUPERVISOR

BRNO 2021

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Student:	**Bc. Milan Marek**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Informační management
Vedoucí práce:	**Ing. Petr Sedlák**
Akademický rok:	2020/21

Ředitel ústavu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává diplomovou práci s názvem:

Návrh zabezpečení herního serveru

Charakteristika problematiky úkolu:

Úvod
Cíle práce, metody a postupy zpracování
Teoretická východiska práce
Analýza současného stavu
Vlastní návrhy řešení
Závěr
Seznam použité literatury
Přílohy

Cíle, kterých má být dosaženo:

Navrhnout zabezpečení herního serveru připojeného na Internet formou metodiky pro nápravu bezpečnostních slabin.

Základní literární prameny:

ČSN ISO/IEC 27001, Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky, Praha: Český normalizační institut, 2014.

ČSN ISO/IEC 27002, Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Soubor postupů, Praha: Český normalizační institut, 2014.

DOUCEK P., L. NOVÁK a V. SVATÁ. Řízení bezpečnosti informací. Praha: Professional Publishing, 2008. ISBN 80-86898-38-5.

ONDRÁK V., P. SEDLÁK a V. MAZÁLEK. Problematika ISMS v manažerské informatice. Brno: CERM, Akademické nakladatelství, 2013. ISBN 978-80-7204-872-4.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2020/21

V Brně dne 28.2.2021

L. S.

Mgr. Veronika Novotná, Ph.D. ředitel	doc. Ing. Vojtěch Bartoš, Ph.D. děkan

Abstrakt

Tato diplomová práce se zabývá návrhem zabezpečení herního serveru, který je připojen do internetu. Na základě nynějšího zabezpečení a oskenování serveru nástroji k penetračnímu testování je navržena kompletní metodika pro napravení zjištěných bezpečnostních mezer.

Klíčová slova

zabezpečení, nástroj, počítačová síť, porty, firewall

Abstract

This master thesis focus on game server security which is connected directly to the internet. Based on current security and scanning the server with penetration testing tools, I designed complete methodology for fixing security issues and vulnerabilities.

Key words

security, tool, computer network, ports, firewall

Bibliografická citace

MAREK, Milan. Návrh zabezpečení herního serveru [online]. Brno, 2021 [cit. 2021-05-05]. Dostupné z: https://www.vutbr.cz/studenti/zav-prace/detail/133632. Diplomová práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce Petr Sedlák.

Čestné prohlášení

Čestné prohlášení Prohlašuji, že předložená diplomová práce je původní a zpracoval jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským). V Brně dne 5.5.2021

..……..

podpis studenta

Poděkování

Moje poděkování patří především Ing. Petru Sedlákovi. za vedení diplomové práce. Děkuji mu za jeho odborné rady a pomoc při řešení problémů. Za podporu bych chtěl také poděkovat své rodině a přátelům.

OBSAH

ÚVOD

V posledních letech byl ve světě IT technologií kladen důraz spíše na rychlost, ale nevěnovala se dostatečná pozornost zabezpečení. To se nepatrně změnilo k lepšímu v posledním roce, kdy svět zasáhla krize spojená s covid-19 a lidé začali pracovat více ze svých domovů. Musejí se připojovat do firemního prostředí buď prostřednictvím VPN nebo proxy, u čehož musí být zabezpečení na prvním místě. Pokud by nebylo, práce potencionálních útočníků a čas vynaložen na prolomení firemní bezpečnosti by se razantně snížil. Prolomení bezpečnosti může mít pro firmu, popřípadě provozovatele fatální důsledky, útočník může ukradnout citlivá data, poškodit je nebo využít výpočetní výkon zařízení k útokům na další zařízení.

Problémy, které souvisí se zabezpečením můžeme vidět každý den kolem nás. Jsou to zprávy o výpadcích sítě v nemocnicích, útocích na webové stránky vládních institucí, napadení sítě různých společností nebo třeba nefunkčnost rezervačních systémů. Pravděpodobnost, že útoky úplně vymýtíme je nulová, ale pro jejich minimalizaci by měl každý dodržovat určitá pravidla a zabezpečovat si svá zařízení.

CÍLE PRÁCE, METODY A POSTUPY ZPRACOVÁNÍ

Cílem této diplomové práce je zabezpečení funkčního herního serveru pomocí firewallových pravidel a technik penetračního testování, jako jsou skenování portů nebo brute force útoky na služby, běžící na herním serveru. Poté vytvořím podrobný návod s instrukcemi pro zabezpečení zjištěných nedostatků a zranitelností.

Testování budu provádět primárně z virtuálního zařízení s operačním systémem kali linux, který je vyvíjený společností Offensive Security právě za účelem penetračního testování a má v sobě některé potřebné nástroje již nainstalované. Kali linux je založen na linuxovém jádru debianu.

Všechna data a výstupy budou uchovávána v takové podobě, aby byla dostatečně čitelná, ale také zabezpečená. K těmto datům by se neměl dostat nikdo jiný, jelikož by mohla vést ke kompromitaci daného serveru. Z tohoto důvodu nebudu v diplomové práci uvádět reálné IP adresy a doménové názvy.

Všechny skeny a útoky půjdou z vnější sítě – internetu z důvodu co nejpřesnější simulace potencionálních hrozeb.

1 TEORETICKÁ VÝCHODISKA PRÁCE

V této části se zabývám technologiemi a základními pojmy, které jsou nezbytné pro zpracování analytické a praktické části diplomové práce.

1.1 ROZDĚLENÍ SÍTĚ PODLE ROZSAHU

Sítě se dělí podle několika kritérií, ve většině situací je však dělíme podle rozsahu, a to na PAN, LAN, MAN A WAN.

Jako přenosové médium se u všech těchto sítí můžou použít optické či metalické kabely, popřípadě rádiové spoje – elektromagnetické vlny. S optickými trasami se setkáváme spíše u LAN a větších sítí.

1.1.1 Personal Area Network (PAN)

Jako osobní síť si můžeme představit jakoukoliv síť na malém prostoru. Jedná se například o několik zařízení, které jsou propojené pomocí USB nebo Bluetooth. Může jít také o propojení mezi počítačem a webovou kamerou, audio doplňky nebo třeba mobilním telefonem.

1.1.2 Local Area Network (LAN)

Tyto sítě jsou určeny pro jedno lokální místo, může jít třeba o podnik, jednu budovu nebo místnost. V síti LAN se zajišťuje sdílení lokálních prostředků, mezi které se řadí tiskárny, data a aplikace [2].

Co se týče konkrétní rozlohy, tyto sítě se mohou pohybovat v rozmezí desítek až stovek metrů.

1.1.3 Metropolitan Area Network (MAN)

MAN je síť v rámci jednoho města, případně určité části města. Může dosahovat délky několika desítek kilometrů a propojuje několik různých LAN sítí. Jedná se většinou o přístupové sítě do internetu.

1.1.4 Wide Area Network (WAN)

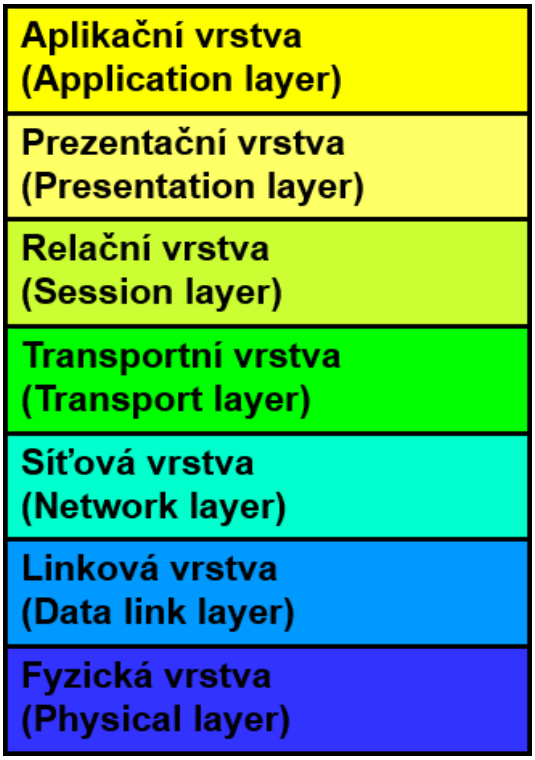
Jedná se o rozsáhlé sítě, ve kterých jsou spojovány sítě LAN. Spojování těchto sítí se provádí speciálními linkami, ale spojení může být i bezdrátové. Do těchto sítí mohou spadat městské sítě, ale klidně i celosvětové – internet. Rozlohou tedy nelze přesně definovat, jelikož nemá omezení [2].

1.2 REFERENČNÍ MODEL ISO/OSI

Úkolem referenčního modelu ISO/OSI je pochopení komunikace, která probíhá po síti. Daný model dělí síťovou komunikaci do sedmi vrstev. Každá vrstva má svoji definici a pravidla. Informace se v rámci modelu předávají pouze mezi sousedními vrstvami. Reálné modely, které se v dnešní době používají vycházejí z logiky ISO/OSI modelu.

Princip ISO/OSI modelu je v tom, že nižší vrstva předá informaci vyšší vrstvě, ta ji zpracuje a dále předává vrstvě nadřazené. Tato spolupráce je věcí výrobce sítě, model doporučuje i horizontální spolupráci. Je žádoucí, aby dvě stejné vrstvy mezi různými sítěmi uměly spolupracovat a komunikovat [2].

- Vznikl „shora“ a byl vnucen uživatelům
- Většina předpokladů časem pozbyla na platnosti
- Je příliš rozsáhlý, tvůrci modelu do něj zahrnuli vše, co by mohlo být někdy k užitku
- Řešení, která byla navržena jsou z praktického hlediska těžkopádná až nerealizovatelná [1]



Obrázek 1 Vrstvy referenčního modelu ISO/OSI

[Zdroj: 1]

1.2.1 Fyzická vrstva

Fyzická vrstva popisuje, jak jsou řešeny mechanické a funkční vlastnosti, například jakým signálem se reprezentuje logická jednička, přijímání začátku bitu, tvar konektoru nebo k čemu je použit v kabelu daný vodič [2].

Jednotkou této vrstvy je bit a pracuje na bázi přijmi bit, odešli bit. V této vrstvě neprobíhá žádná adresace a bity jsou odesílány přes přenosová média k jakémukoliv příjemci. Přenosový protokol je závislý na přenosovém médiu a prostředí.

1.2.2 Linková vrstva

Linková vrstva slouží k přenosu informací po fyzickém médiu. Na rozdíl od fyzické vrstvy zde již probíhá adresace a pracuje s fyzickými adresami síťových karet. Linková vrstva má za úkol přijímat a odesílat rámce. Kontrolují se cílové adresy každého z přijatých rámců a určuje, zda je možné předat rámec vyšší vrstvě [2].

Linková vrstva má jako jednotku datový rámec, který přenáší k uzlům v dosahu svého přenosového média. Synchronizace zařízení probíhá na úrovní rámců a pokud je třeba, zajišťuje se spolehlivost. Vrstva řídí tok dat, aby nedošlo k zahlcení a adresuje na lokální úrovni.

1.2.3 Síťová vrstva

Slouží ke komunikaci a směřování mezi dvěma aktivními prvky nebo sítěmi, mezi kterými ještě neexistuje přímé spojení. Protože mezi uzly zpravidla bývá více možných cest spojení, tato vrstva má také na starosti volbu trasy při komunikaci. Tento krok nazýváme směrováním, nebo-li routingem [2].

Jednotkou přenosu této vrstvy je paket. Síťová vrstva nabízí možnost přenosu paketu k jakémukoliv uzlu na světě. Přenos může probíhat přes libovolný počet mezilehlých uzlů. Adresace probíhá na globální úrovni.

V síťové vrstvě se dnes používají adresace skrze internet protokol. Tento protokol využívá dvě hlavní verze – IPv4 a IPv6. Dnes je stále nejpoužívanější verze IPv4, ale pomalu se ji vytlačuje IPv6 z důvodu počtu adres. IPv4 adresy jsou 32 bitové a dělí se do tříd.

Třída	Adresní rozsah
Třída A	0.0.0.0 – 127.255.255.255
Třída B	128.0.0.0 – 191.255.255.255
Třída C	192.0.0.0 – 223.255.255.255
Třída D	224.0.0.0 – 239.255.255.255
Třída E	240.0.0.0 – 255.255.255.255

Tabulka 1 Rozdělení IP adres do tříd

[Zdroj: 3]

IP adresy se dělí do dvou skupin, a to na privátní a veřejné. Privátní adresu nám přiřadí například domácí router nebo domácí DHCP server. Tyto adresy jsou potom překládané routerem pomocí „NATovacích“ pravidel pro přístup do internetu. Dvě zařízení v různých sítích mohou mít stejnou privátní IP adresu, ale nemělo se stát, že mají stejnou veřejnou adresu. To by potom mohlo vést k MITM (Man In The Middle) útoku. Privátní adresy mají podle standardu vymezený určitý rozsah:

- 10.0.0.0 – 10.255.255.255
- 127.0.0.0 – 127.255.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 – 192.168.255.255 [3]

1.2.4 Transportní vrstva

Transportní vrstva dělí přenášené zprávy na pakety a potom je opět skládá zpátky na zprávy. Pří přenosu je určité riziko, že se některé pakety ztratí nebo pomíchají [2].

Jednotkou je u této vrstvy datagram. Probíhá zde transport datagramu mezi procesy dvou uzlů a přizpůsobuje se charakteru přenosu a potřebám aplikací. Tvoří se zde spolehlivý přenos z nespolehlivého a zároveň se z nespojovaného stává přenos spojovaný, čímž se vytváří spojení nebo-li session.

Transportní vrstva má dva hlavní protokoly, těmi jsou TCP a UDP.

TCP

Protokol TCP je spojově orientovaný a spolehlivý. Předtím než uzly navážou spojením přes protokol TCP, musí provést takzvaný handshake. Ten probíhá tak, že si stanoví parametry pro přenos dat. Handshake je třístranný a při navázání jsou vždy vyměněny tři pakety. Zařízení, které se chce připojit ke druhému nejprve naváže spojení tak, že zašle SYN paket. Tento paket říká druhému zařízení, že s ním chce navázat spojení. Druhé zařízení odpovídá paketem ACK – acknowledgement zároveň se SYN. Tím zařízení potvrzuje obdržení dat a dává najevo jakým sekvenčním číslem komunikaci začne. Jako poslední stvrzuje převzetí informací první zařízení paketem ACK, ve kterém jsou potvrzena sekvenční čísla obou zařízení. Pomocí těchto čísel je potom zaručeno, že se žádná data neztratila.

UDP

Protokol UDP je opakem TCP, je nespojovaný a nespolehlivý. Jeho hlavní výhodou je rychlost. Protože nemusí navazovat spojení odpadají určité kontroly. Na straně odesílatele tento protokol odešle data, připíše se do datagramu číslo portu, na který má být odeslán a už ho nezajímá, jestli byl datagram příjemci doručen nebo ne.

1.2.5 Relační vrstva

Úkolem relační vrstvy je navázání a ukončení spojení. Může zde probíhat také ověření uživatelů a zabezpečení přístupu k jednotlivým zařízením [2].

Jednotkou přenosu relační vrstvy je jedno spojení. Nabízí také vedení relace a podporuje transakce. Na úrovni této vrstvy se již neadresuje, jelikož adresace na cílený proces proběhla už ve čtvrté vrstvě, která předává této vrstvě číslo portu, kterým jsou označeny služby. Relační vrstva je nejméně vytížená z celého modelu.

Port

Nejznámějšími porty jsou takzvané well-known porty, přes které se zařízení připojují k určitým službám. Tyto porty relativně zjednodušují spojení, jelikož jsou známy jak příjemci, tak odesílateli. Příkladem takového portu je například port 22, který obsluhuje připojení přes SSH nebo port 80, který zajišťuje službu pro přenos hypertextových dokumentů [4].

Dalším typem portů jsou dynamicky alokované, tyto porty jsou předem definovány a poté jsou přiděleny za běhu systému. Používají se pro síťové služby, až jsou potřeba. Systém pak musí zajistit, aby se stejný port nepřidělil k více službám [4].

Každý port musí být přidělen z rozsahu 0-65535 s tím, že rozsah 0-1023 je rezervován právě pro well-known porty, 1024-49151 jsou porty pro registraci služeb a pro dynamické alokování se využívají porty 49152-65535 [4].

1.2.6 Prezentační vrstva

Úkolem této vrstvy je konverze dat. Přenášená data mohou být v síti šifrovány. Prezentační vrstva také sjednocuje formu přenášených údajů a data komprimuje, popřípadě šifruje. V praxi většinou splývá s relační vrstvou [2].

Prezentační vrstva nemá jednotku a stejně jako u vrstvy relační zde nemá adresace žádný smysl.

1.2.7 Aplikační vrstva

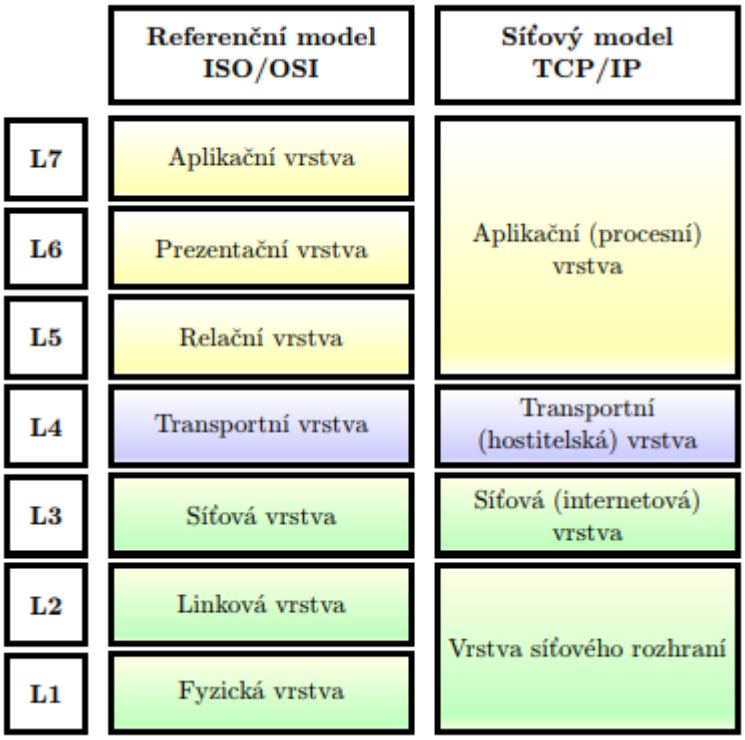
Aplikační vrstva uživatelům zpřístupňuje síťové služby a přístup k souborům u jiných počítačů, správu sítě, elektronické zprávy nebo třeba vzdálený přístup k tiskárnám [2].

Jako u předešlých dvou vrstev zde adresace nemá smysl. Jednotka přenosu zde také není, ale standardizuje části určitých aplikací.

1.3 ARCHITEKTURA TCP/IP

Jelikož je referenční model ISO/OSI příliš složitý a teoretický, vytvořilo se několik zjednodušených variant. Neznámějším z těchto variant je model TCP/IP, který je také známý jako DoD model. Takto se mu říká podle ministerstva obrany USA (Department of Defense) [5].

Síťový model TCP/IP popisuje síťový zásobník TCP/IP, dále popisuje možnost napojení nových protokolů nebo spolupracujících prvků. Oproti ISO/OSI modelu má pouze 4 vrstvy, těmi jsou vrstva síťového rozhraní, která zastupuje fyzickou a linkovou vrstvu, vrstva síťová, transportní vrstva a vrstva aplikační, která zastupuje relační, prezentační a aplikační vrstvu. Model TCP/IP byl navržen tak, aby odolával co nejvíce rizikům, chybám přenosu a podmínkám provozu. Většinu práce přenechává koncovým zařízením, aby bylo jádro sítě rychlé a dalo se spravovat distrubuovaně [5, 6].



Obrázek 2 Srovnání *modelu ISO/OSI a TCP/IP*

[Zdroj: 6]

1.3.1 Vrstva síťového rozhraní

Funkčností zastává fyzickou a linkovou vrstvu ISO/OSI modelu. V TCP/IP nejsou pro tuto vrstvu stanoveny žádné protokoly a je určena pouze pro komunikaci s vyšší vrstvou. Probíhá zde komunikace s hardwarem, případně některá část může být i hardwarově implementována. TCP/IP přijímá kompatibilní architekturu první a druhé vrstvy [5, 6].

V nižších částech může pracovat s jednoduchými zařízeními, příkladem může být třeba hub nebo repeater. Ve vyšších částech potom pracuje se zařízeními pracující s rámci a oddělují jednotlivé segmenty sítě. Mluvíme například o switchi nebo bridgi [5, 6].

1.3.2 Síťová vrstva

Nazývaná také jako internetová vrstva. Probíhá zde propojování sítí a následně jejich směrování. Příkladem zařízení, které pracuje na síťové vrstvě je router nebo L3 switch [6].

Do síťové vrstvy můžeme zařadit směrovací protokoly, jako jsou OSPF, EIGRP, RIP, BGP a jim podobné [5, 6].

K rozšířenějším protokolům patří například ICMP, který slouží k jednoduchému spojení mezi zařízeními v síti. Protokol je primárně využíván pro ověření, jestli je nějaké zařízení online pomocí pingu [5, 6].

1.3.3 Transportní vrstva

Jádro transportní vrstvy tvoří protokoly TCP/UDP, které jsem popsal u transportní vrstvy referenčního modelu ISO/OSI.

1.3.4 Aplikační vrstva

Aplikační neboli procesní vrstva v sobě sdružuje 3 nejvyšší vrstvy ISO/OSI modelu. Je zde také velké množství protokolů a většinou komunikují s aplikacemi, které přistupují do sítě. Příkladem jednoho takového protokolu je http, který je mimo jiné využíván webovými prohlížeči [5, 6].

Dalším příkladem protokolu aplikační vrstvy je SMTP, IMAP nebo POP3, které se starají o příjem a odesílání elektronické pošty. Na rozdíl od nižší vrstvy, aplikační vrstva neřeší TCP/IP protokoly, ani jejich činnosti.

1.4 ETHERNET

V modelu ISO/OSI ethernet reprezentuje fyzickou a linkovou vrstvu. Základním znakem ethernetu může být přístupová metoda CSMA/CD. Specifikace ethernetu se zabývají použitím topologie nebo kabelu. Díky rozšířenosti ethernetu je zde dostupné velké množství aktivních prvků, které se dají použít při instalaci [2].

Při tvorbě sítě je nutné dodržovat určitá pravidla, jako jsou třeba délka segmentů, topologická pravidla nebo délku sítě. U kolizní domény je předpoklad, že se signál šíří nekonečnou rychlostí a pokud začne vysílat na jedné stanici, je okamžitě slyšet na druhé. To však není fyzikálně možné, a proto máme stanoveny maximální vzdálenosti linky, na kterých bude CSMA/CD fungovat. Pro maximální rozměr sítě používáme termín kolizní doména [2].

Označení ethernetu má určitá pravidla:

- První číslice vyjadřuje rychlost, se kterou standard pracuje
- BASE popisuje signalizační metodu
- Písmeno na konci určuje typ kabelu, kdy F značí optický (Fiber) a T metalický kroucený (Twisted)

1.4.1 Ethernet (Rychlost do 10 Mb/s)

Dnes se již nepoužívá, dosahoval rychlosti 10Mb/s, což v dnešní době nedostačuje. Měl 5 variant, a to 10 BASE-5, 10 BASE-2, 10 BASE-T, 10 BASE-F a 10 BASE-FB

1.4.2 Fast ethernet (Rychlost do 100 Mb/s)

Dnes ještě stále rozšířená norma použití ethernetu. Odpovídá doporučení IEEE 802.3. Je to metoda založená na CSMA/CD, s tím rozdílem, že oproti ethernetu pro 10 Mb/s se nedá vést koaxiálním kabelem. U tohoto standardu se rozlišují 3 varianty, 100 BASE-TX, ve které se využívá nestíněné kroucené dvojlinky páté kategorie s využitím dvou párů, 100 BASE-FX, což je standard pro optické kabely a 100 BASE-T4, což je starší norma a používá se zde kroucena dvojlinka třetí a čtvrté kategorie s využitím všech čtyř párů [2].

1.4.3 Gigabitový ethernet (Rychlost do 1 000 Mb/s)

Dnes asi nejrozšířenější forma, je standardizována pro kroucenou dvojlinku a optické kabely. Dělí se na standard 1000 BASE-X, který je určený pro optické kabely, a ještě je dělený na 1000 BASE-SX, kde je zdrojem LED dioda nebo laser s vlnovou délkou 850 nm a 1000 BASE-LX, kde se používá pouze laser s vlnovou délkou 1 310 nm a můžeme jej využít na větší vzdálenosti než SX. Ke standardu 1000 BASE-X je zde také 1000 BASE-T, který je určen pro metalické kabely. Používá se zde čtyř-párová kroucená dvojlinka kategorie 5e. Změnou oproti pomalejším standardům je, že se používají všechny čtyři páry vodičů [2].

1.4.4 10 Gigabitový ethernet (Rychlost do 10 Gb/s)

Je to norma, která se používá spíše k páteřním vedení společností. Přenosovým médiem bývá v drtivé většině optický kabel a může být použita v sítích LAN, MAN i WAN. Délka

může dosahovat až 40 km. Pro tuto normu se používají 3 standardy – 10GBASE-SR, která je na krátké vzdálenosti a používá se zde mnoho vidový kabel. Dalším standardem je 10GBASE-LX4, u tohoto standardu je možná vzdálenost s mnoho vidovým kabelem až 300 metrů, s jedno vidovým kabelem je to až 10 km. Posledním standardem je 10GBASE-LR/ER, pracují s jedno vidovými vlákny a přenosová vzdálenost může dosahovat až 40 km [2].

1.4.5 40 Gigabitový ethernet a 100 Gigabitový ethernet

Tato norma není dostupná širší veřejnosti, využívá se spíše jako páteřní síť ve větších datových centrech.

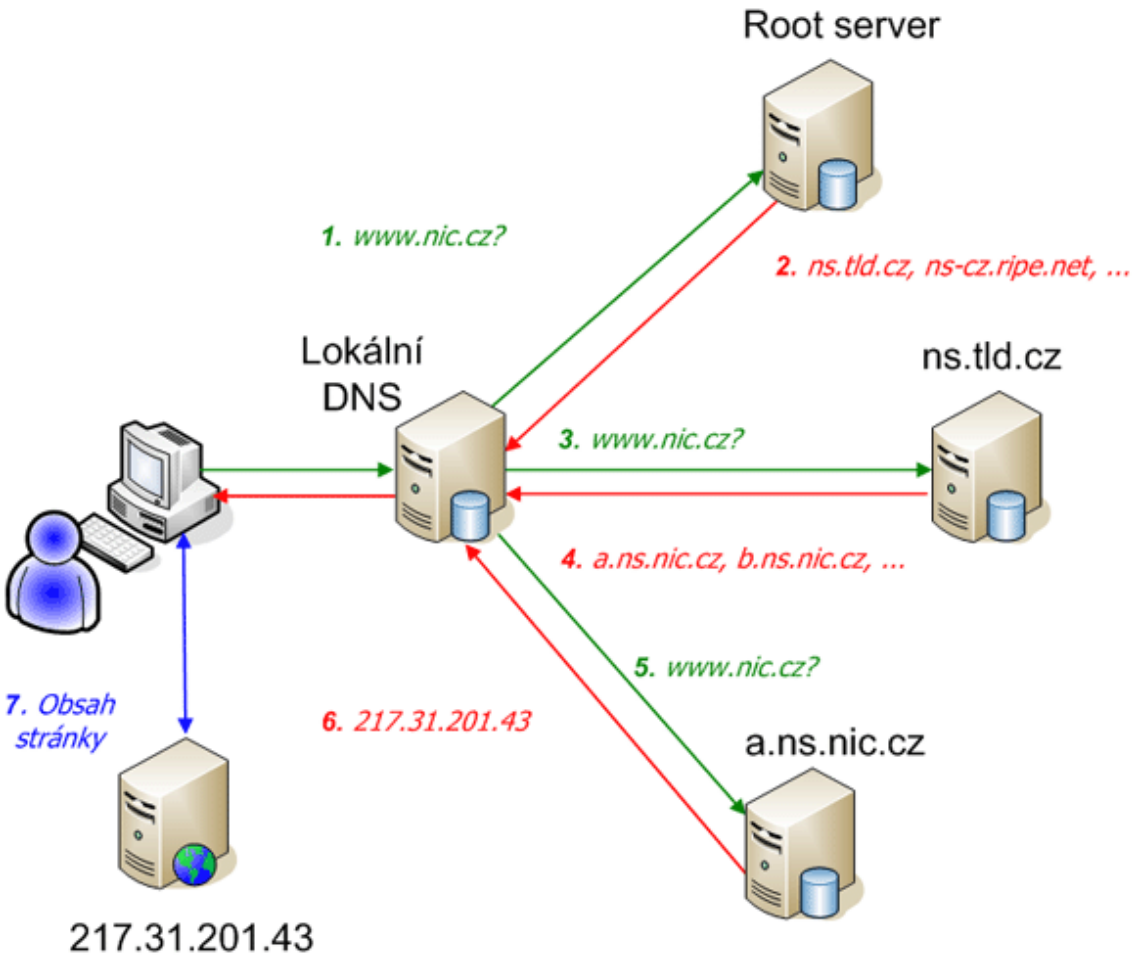
1.5 SERVER A JEHO SLUŽBY

Serverem je myšlena fyzická nebo virtuální stanice, na níž jsou nainstalovány služby, které obsluhují další zařízení v síti. Každá počítačová síť by měla mít server, a tudíž můžeme říct, že je jádrem počítačové sítě. Server musí být dostatečně výkonný, aby zvládnul obsluhovat mnoho požadavků jednotlivých stanic a zároveň, aby mohl zaručit zabezpečení uložených dat. Na hardware jsou tedy kladeny mnohem vyšší požadavky než u klasických koncových zařízení [7].

1.5.1 DNS

DNS nebo-li domain name server je jednou ze základních služeb. Abychom si nemuseli pamatovat IP adresy každého zařízení, je tady právě DNS, který překládá doménové jména na IP adresy.

Každé zařízení má nastavené lokální DNS, ten obdrží dotaz o zadaném hostovi, pokud o něm nemá žádné informace, posune dotaz dál na autoritativní server. Tento server má za úkol uchovávat přesné informace o doménách. Jakmile autoritativní server odpoví na dotaz, lokální DNS si informace uloží do cache pro případ stejného dotazu v budoucnosti. Záznamy v cache mají určitý TTL, aby se paměť nezahlcovala přebytečnými informacemi. Na následujícím obrázku je zobrazen příklad dotazů na doménové jméno pomocí DNS.

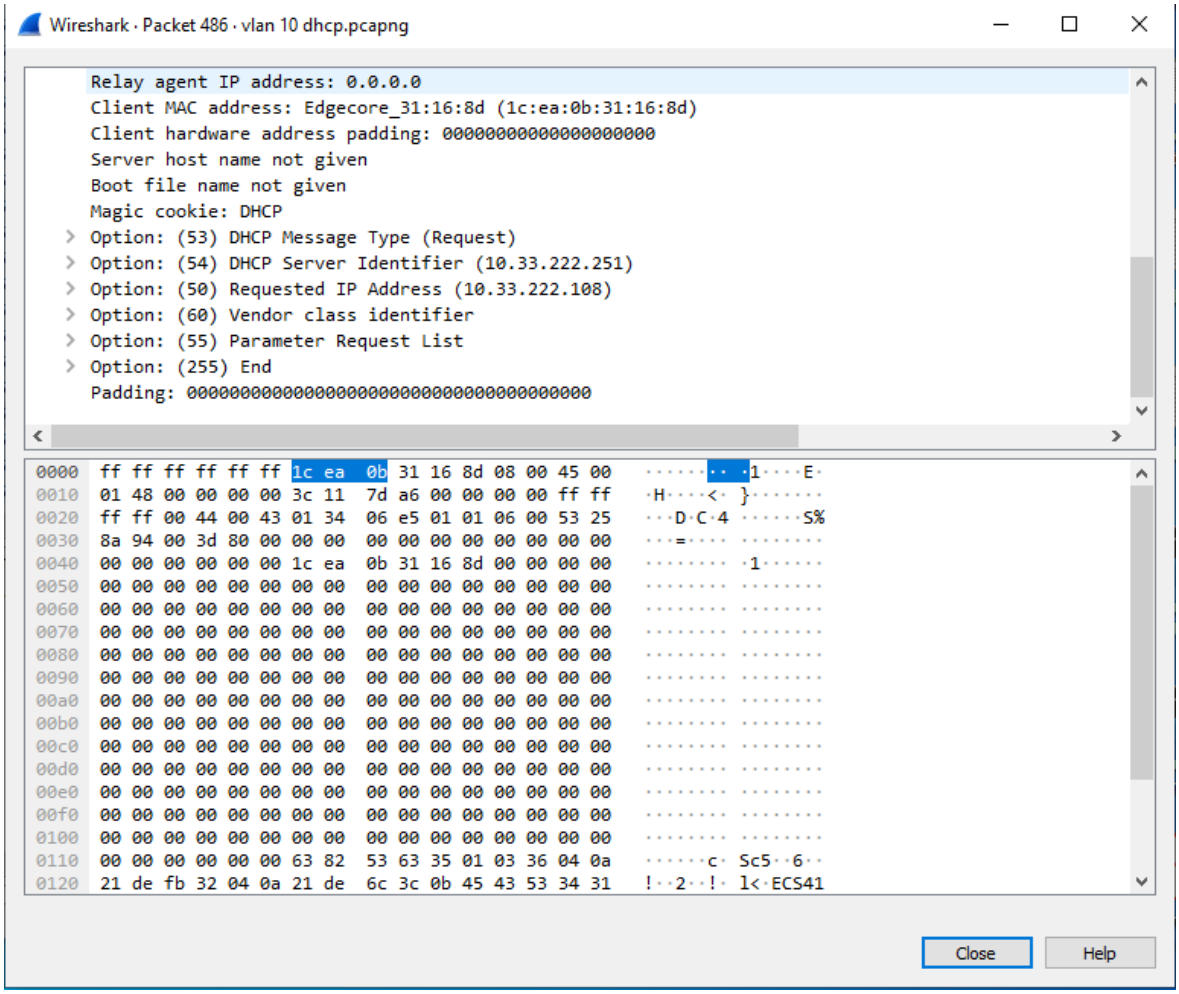


Obrázek 3 Postup při dotazování na neznámý doménový název pomocí autoritativního serveru CZ.NIC

[Zdroj: 8]

1.5.2 DHCP

Po připojení klienta do sítě zařízení vyšle broadcastem takzvaný DHCP Discover paket. To znamená, že tento paket je doručený na všechna zařízení, která jsou v síti. Na tento paktet potom odpoví DHCP server paketem DHCP offer, který nabídne klientovi IP adresu, zároveň s informací o výchozí bráně, subnet masce a podobně. Následně klient pošle DHCP request, kterým o tuto konfiguraci zažádá. Po této žádosti DHCP server zasílá paket DHCP ack, kterým potvrzuje přidělení konfigurace klientovi.



Obrázek 4 Příklad DHCP request paketu

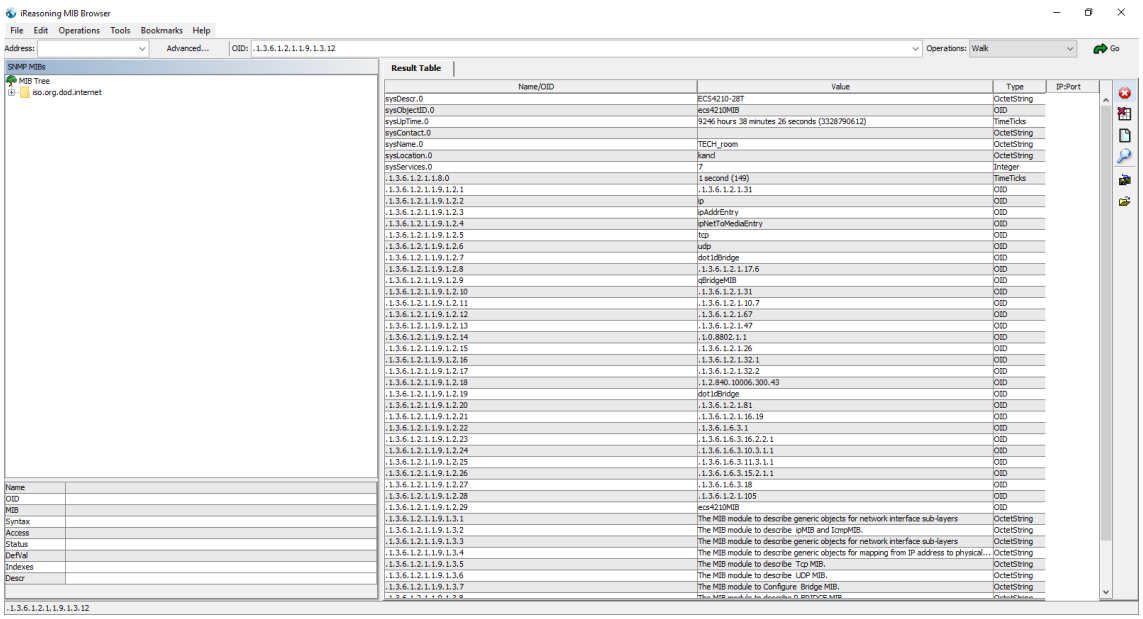
[Zdroj: vlastní zpracování]

1.5.3 TFTP

Trivial transfer protokol je jednodušší verzí k FTP, který slouží pro přenos dat. TFTP mohou zařízení použít k nabootování ze sítě. Rozdílem oproti FTP je, že používá nezabezpečeného protokolu UDP, zatímco FTP používá TCP. Výhodou může být rychlejší odezva, avšak problém je v tom, že TFTP nevyužívá žádné autentikace, tudíž jsou všechny soubory dostupné komukoliv, kdo si o ně zažádá. Autentikace není implementována, protože při implementaci se počítalo s tím, že vstup z internetu do lokální sítě je vysoce nepravděpodobný. S dobou VPN a proxy serverů je ale toto řešení často využívané, a proto není v některých případech použití TFTP úplně bezpečné [4].

1.5.4 SNMP

SNMP nebo-li simple network management protokol je protokol, pomocí kterého si dvě zařízení v síti předávají informace. Dovoluje zařízením komunikovat, i když jsou od jiného výrobce nebo hardwarově rozdílné. Protokol se využívá především k monitorování a managementu určitého zařízení, například switche nebo routeru. Pro práci se zařízením přes SNMP jsou potřeba takzvané MIB soubory, které obsahuji ke každému segmentu unikátní OID, podle kterého můžeme nastavit určitou funkci nebo najít hledanou hodnotu. Pro monitoring zařízení se využívá softwaru třetí strany, který informace zpracuje a následně z nich dokáže udělat statistiky.



Obrázek 5 Příklad výčtu informací pomocí SNMP přes MIB browser

[Zdroj: vlastní zpracování]

1.5.5 NTP

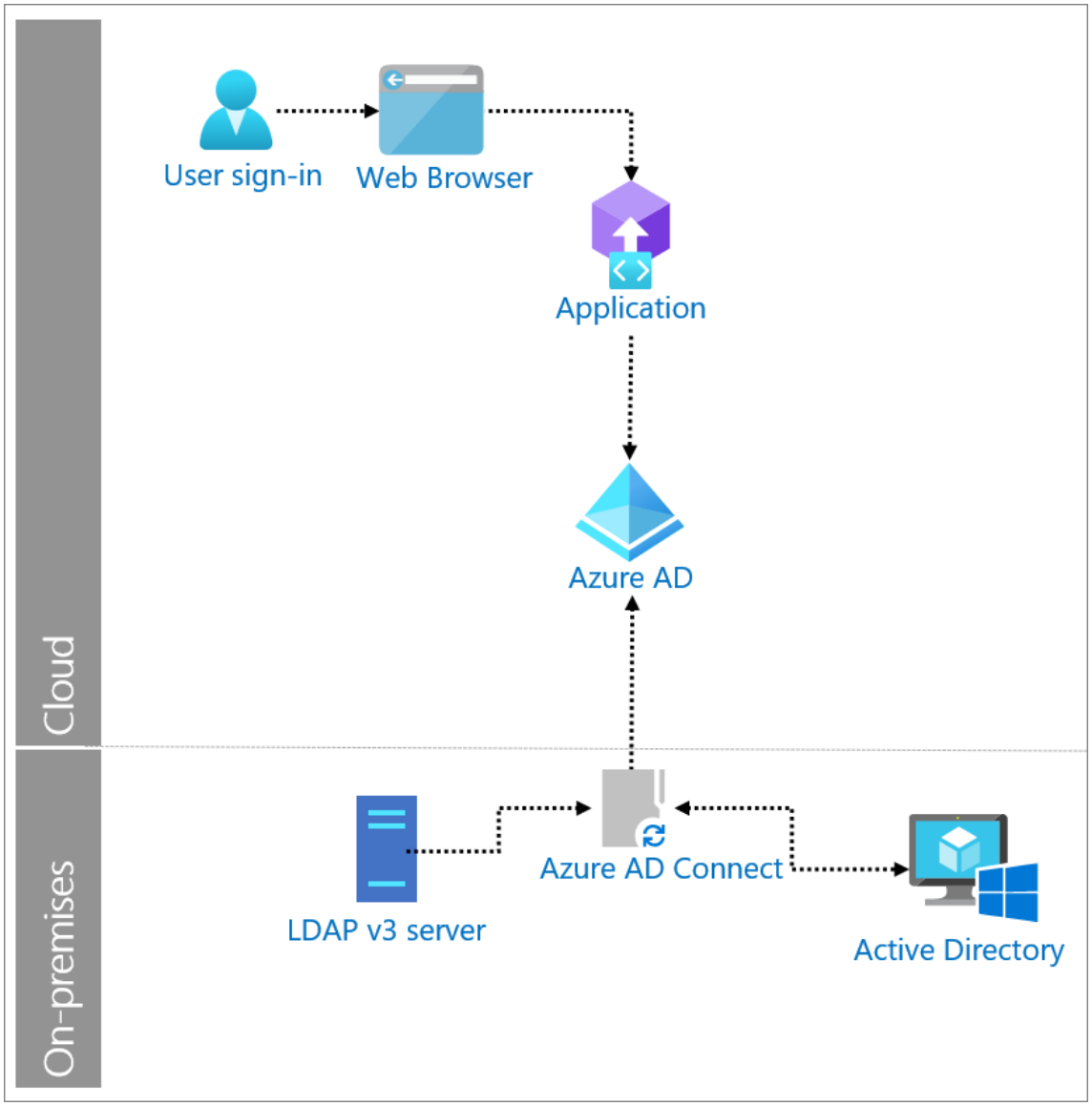
NTP je protokol pro synchronizaci času mezi síťovými zařízeními. Tento protokol se využívá pro přesnost logů, ale také se může využít například pro autentizaci. Je dobrý k získávání informací, ale může být zneužit potencionálními útočníky pro kolekci informací jako uptime systému, statistiky z paměti nebo třeba čas serveru.

1.5.6 LDAP

LDAP je zkratka pro protokol popisující ukládání a přístup k datům na adresářových serverech, na které přistupuje více uživatelů. Tyto uživatele je třeba oddělovat a požadovat po nich autentizaci, aby nedošlo k neoprávněnému přístupu k datům. Takováto oprávnění by měly být udržovány v jednoduše upravitelné podobě.

Komunikace začíná zasláním požadavku klientem na port 389 požadovaného serveru, čímž naváže spojení. Na to server odpovídá klientovi požadavkem o konkrétní informaci, případně set informací. Následně server vyhodnocuje, zda má klient k požadovaným datům přístup a klientovi zašle odpověď [9].

Pomocí LDAP se můžeme připojovat i k AD, které je fyzicky v jiné lokaci. K tomuto kroku ale potřebujeme nějakou aplikaci či program. Příkladem může být připojení k AD pomocí Azure AD viz. obrázek.



Obrázek 6 Připojení uživatele k „on-premises“ active direktory skrze protokol LDAP

[Zdroj: 10]

1.5.7 NETBIOS

NETBIOS je program, který byl vytvořen na začátcích vývoje PC sítí. Umožňuje aplikacím komunikovat na různých počítačích v rámci LAN sítě. NETBIOS je zabudován v balíčku SMB, který je instalován na všech zařízeních se systémem Windows a může být doinstalován i do unixových systémů. Tento balíček umožňuje spojení dvou PC v síti. Služby, které jsou dostupné přes NETBIOS musí být dobře zabezpečené, jelikož

představují bezpečnostní riziko. Nyní se využívá SMB verze 3, jelikož první 2 verze obsahovali bezpečností zranitelnosti.

1.5.8 Portmap

Jelikož ne všechny portu služeb jsou předem rezervovány, portmapper má za úkol registrovat jednotlivé porty při spuštění RPC služby. Je to program, který ukládá čísla použitých portů. Výpis těchto portu je na vyžádání zaslán klientovi. Tento výpis obsahuje také seznam používaných služeb. Výpis obsahuje mnoho informací, které se dají útočníkem lehce zneužít [4].

1.5.9 Simple Service Discovery Protocol

Tento protokol je využíván většinou zařízení v naší domácnosti. Také byl využit při tvorbě protokolu Universal Plug and Play. Je určený spíše pro použití v menších sítích. V principu, pokud se připojí zařízení k síti, může si zažádat o určité informace o připojených prvcích, ale i přímo o dané síti. Toto samozřejmě představuje i určité riziko, jelikož verze simple service discovery protokolu je nezabezpečená a je možno ji jednoduše zneužít k útoku [11].

1.6 NMAP

Nmap, neboli Network Mapper je open source nástroj pro skenování sítě a bezpečnostní audit. Administrátoři využívají nmap také ke správě upgradu služeb nebo třeba k monitorování určitého zařízení. Nmap používá neupravené IP pakety takovým způsobem, aby zjistil, jaké zařízení jsou v síti, jaké používají služby, jaký mají operační systém, jaký používají firewall/paket filter a mnoho dalších užitečných informací. Tento nástroj byl vytvořen pro skenování velkých sítí, ale samozřejmě zvládne oskenovat i jednoho hosta. V balíčku Nmap jsou zahrnuty i další nástroje, jako Ncat, který slouží k debuggingu, Ndiff pro porovnání více výsledků skenů nebo Nping pro analýzu [12].

Nmap umí pomocí argumentů využívat mnohých utilit a zasílat různé typy paketů, používat skripty, nastavit přesné porty, které se mají skenovat a mnoho dalších funkcí.

Následně krátce popíši vybrané přepínače v nástroji nmap:

- **iL** – definuje soubor, ve kterém je seznam IP adres zařízení, které chceme skenovat
- **Pn** – slouží pro optimalizaci skenu, konkrétně přeskočí fázi, která zjišťuje, zda je cílové zařízení online. Tento argument může ušetřit čas při skenování větší sítě
- **sS** – TCP SYN sken, jedna z technik skenování. S cílovým zařízením komunikuje tak, že mu posílá SYN pakety na určité porty.
- **p** – definuje porty, které budou skenovány
- **F** – rychlý mód, skenuje méně portů (nejvíce používané), je tedy méně přesný, ale rychlejší
- **sV** – ověří služby, které běží na daných portech a zobrazí informaci o jejich verzi
- **O** – zapne detekci OS. Detekce systému nemusí být vždy přesná
- **f** – fragmentuje pakety. Používá se, pokud chceme, aby ochrana koncového zařízení sken nedetekovala
- **S** – zamění zdrojovou IP adresu
- **A** – zapne agresivní skenování. Získané informace jsou detailnější, ale nevýhodou je, že skenování zanechá hodně stop na cílovém zařízení a lehce jej lze odhalit
- **script** – argument, který dovoluje použít skripty jak zabudované, tak ty, které byly napsány třetí stranou. Tato funkce je jedna z nejpodstatnějších v celém nmapu, jelikož si díky ní můžeme upravit sken podle potřeb.

1.7 ANALÝZA RIZIK

Analýza rizik je proces, při kterém definujeme hrozby, jaká je pravděpodobnost, že se hrozba uskuteční a jaký by byl její dopad. Pokud chceme řešit problém v jakékoliv oblasti, je dobré analýzu rizik udělat, jelikož potom může být vstupem pro řízení zjištěných rizik [13].

1.7.1 Hrozba

Hrozba je určitá událost, která má negativní dopad na aktiva, případně celkově na chod serveru a mohla by ohrozit jeho další chod. Hrozby můžou být různé, mohou mít přírodní nebo lidský původ a také mohou být náhodné či úmyslné. Také můžou být interní nebo externí hrozby [13].

1.7.2 Lewinův model

Pokud chceme provádět nějaké změny v organizační struktuře, můžeme použít například Lewinův model. Tento model získal jméno podle amerického psychologa Kurta Lewina a probíhá ve třech fázích. První fází je rozmrazení současné úrovně, jinými slovy určitá příprava na změnu, další fází je přechod na novou úroveň čili fáze změny a poslední je znovuzmrazení nové úrovně nebo-li fixace provedené změny.

2 ANALÝZA SOUČASNÉHO STAVU

Ve druhé části krátce představím server, pro který návrh bezpečnosti sestavuji, popíši aktuální stav a zanalyzuji slabé stránky serveru. V této kapitole také provedu analýzu rizik, abych mohl určit, jaký dopad by měly různá rizika a také, na jaké rizika je nutné se zaměřit primárně.

2.1 SERVER THESIS MU

Na herním serveru, kterému jsem dal název Thesis MU, běží hra MU online. Název serveru je smyšlený, jelikož v práci popisuji bezpečnostní rizika, programy a služby, které na serveru běží. Tyto informace není dobré veřejně vystavovat, jelikož by to mohlo mít na chod serveru negativní vliv.

Hra MU online je korejské free to play MMORPG a byla vydána v roce 2003. Společnost Webzen, která tuto hru vydala na ni stále pracuje a vydává updaty. Větší updaty jsou ve formě sezón a menší ve formě epizod. Tyto aktualizace do hry přidávají nové prvky, postavy, ale i různé soutěže či události.

Historie tohoto projektu sahá do roku 2010, kdy jsem poprvé herní server spustil. Server je hostovaný nejmenovanou společností v Německu. Měl několik výpadků a pauz, ale za těchto téměř 11 let se na serveru vystřídalo až 15 tisíc hráčů. Server prošel mnoha sezónami a dříve byl orientován pouze na československou komunitu. Zde byl považován za jeden z nejlépe nastavených CZ/SK serverů. Poté se ale zaměření přesunulo na evropskou scénu, kde si našel také své příznivce, ale z důvodu vysoké konkurence zde nebyl tak úspěšný.

2.2 ANALÝZA RIZIK

V této kapitole popisuji rizika, která momentálně ohrožují bezpečnost serveru, na kterém je hra provozována. Na základě této analýzy poté budou navržena opatření, která by měla snížit pravděpodobnost i dopad rizika. V následující tabulce tyto pravděpodobnosti i dopad slovně popisuji.

Hodnota	Pravděpodobnost	Dopad
0-2	Velmi nízká	Téměř žádný
3-4	Nízká	Malý
5-7	Střední	Střední
8-10	Vysoká	Velký

Tabulka 2 Ohodnocení pravděpodobnosti a dopadu hrozeb

[Zdroj: vlastní zpracování]

Další tabulka slovně popisuje ohodnocení hrozeb podle výsledné hodnoty.

Hodnota	Slovní ohodnocení
0-14	Velmi nízká úroveň hrozby
15-29	Nízká úroveň hrozby
30-44	Střední úroveň hrozby
45-60	Vysoká úroveň hrozby
60 a více	Extrémně vysoká úroveň hrozby

Tabulka 3 Ohodnocení úrovně hrozby

[Zdroj: vlastní zpracování]

Nyní popíšu potencionální hrozby, které mohou server ohrozit. Poté v tabulce spočítám hodnotu hrozby na základě její pravděpodobnosti a případného dopadu.

Neschopnost detekce zranitelnosti

Neschopnost detekce zranitelnosti znamená, že i přes různorodé testy zabezpečení nejsme schopni danou zranitelnost odhalit a odstranit. Toto riziko může mít několik příčin, jednou z nich může být nedostatek času administrátorů nebo třeba nedostatek financí pro zaplacení externí firmy, aby testy provedla. Opatřením může být lepší časový plán pro správu serveru.

Otevřený nežádoucí port

Pro provoz herního serveru musí být otevřené určité porty, přes které se hráči napojují. Jsou to ale specifické porty a pouze ty by měly zůstat otevřené. Pokud zůstane otevřený

port, který využívá některou ze služeb systému Windows, může být zneužit pro útok na tuto stanici.

Neaktualizovaný operační systém

Každý týden je k dispozici několik zero-day zranitelností, které musí výrobci systémů nějakým způsobem záplatovat, některé zranitelnosti jsou méně kritické, některé více. Prioritou by měl být ale aktualizovaný operační systém, jelikož díky těmto zranitelnostem se mohou potencionální útočníci jednoduše dostat do sítě a zkompromitovat server.

Neaktualizované služby a aplikace třetích stran

Stejně jako u operačního systému představuje užívání zastaralých služeb a aplikací velké riziko. Jelikož jsou zranitelnosti vystavovány veřejně a může si je najít kdokoliv, použití těchto zastaralých verzí může vést při objevení k okamžité kompromitaci.

Neschopnost zabezpečení zranitelností

Pokud objevíme nějakou zranitelnost, je třeba ji okamžitě zabezpečit. Za neschopnost zabezpečení zranitelnosti považujeme stav, kdy o slabině víme a nejsme schopni ji zabezpečit.

Využití zranitelnosti otevřeného portu

Jak již bylo uvedeno dříve, pokud je otevřen nežádoucí port nebo nemáme ochráněny porty, popřípadě zapnutý firewall, může dojít k průstupu do sítě pomocí zranitelnosti tohoto otevřeného portu.

Právní postihy z důvodu nezabezpečení serveru

Pokud by došlo ke kompromitaci serveru a ten byl poté zneužíván pro ilegální činnosti, může dojít k upozornění příslušnými orgány. Pokud bychom tyto upozornění ignorovali, mohlo by dojít i k právnímu postihu.

Špatná interpretace stavu zabezpečení

Pokud již máme nějaký způsob, jak detekujeme zranitelnosti v systému, je třeba tyto informace zpracovávat a nějakým způsobem interpretovat, aby mohlo dojít k jejich

omezení, případně eliminaci. Tento stav nastane tehdy, pokud není pověřená osoba schopná správně informace vyhodnotit.

Ztráta důvěry následkem prolomení zabezpečení

Jestli dojde k prolomení zabezpečení a následné kompromitaci serveru, může dojít u hráčů ke ztrátě důvěry a poškození dobrého jména serveru, což může vyústit ve snížený počet hráčů. Tím pádem server ztrácí na atraktivitě.

Ztráta přístupu k serveru

Ztrátou přístupu k serveru se rozumí to, když nebudeme mít možnost se k serveru jakýmkoliv způsobem připojit. Může jít o blokaci IP adres na základě geolokace nebo špatně nastavená pravidla ve firewallu.

Zašifrování dat ransomware útokem

Jelikož k serveru přistupuje i omezený počet lidí, kteří nemají o bezpečnosti větší povědomí, je zde možnost zanesení viru, který může napadnout a zašifrovat veškerá data uložená na serveru.

Nedostatek prostoru pro detekci slabin

Částečně souvisí s první hrozbou. Může k němu dojít v případě, že mají pověřené osoby na práci jiné věci a nemohou se soustředit na detekci těchto slabin. K této hrozbě může dojít i když jsou osoby dostatečně zaškolené a jsou schopné tyto zranitelnosti eliminovat a potencionálnímu útoku zamezit.

Odstavení serveru

Rozumí se tím odstavení serveru například vlivem DDoS útoku, kdy se na server hráči buď nemohou připojit vůbec nebo s vysokou latencí, což hráčům znepříjemňuje hru a snižuje to jejich spokojenost se serverem.

Únik osobních údajů

Následkem špatného zabezpečení může být únik osobních údajů hráčů, které jsou umístěny v databázi na serveru. Osobními údaji jsou myšleny emailové adresy, jména a hesla účtů.

ID	Popis hrozby	Míra pravděpodobnosti	Dopad	Hodnota hrozby
1	Neschopnost detekce zranitelnosti	6	5	30
2	Otevřený nežádoucí port	4	6	24
3	Neaktualizovaný operační systém	3	7	21
4	Neaktualizované služby a aplikace třetích stran	2	7	14
5	Neschopnost zabezpečení zranitelnosti	5	6	30
6	Využití zranitelnosti otevřeného portu	5	8	40
7	Právní postihy z důvodu nezabezpečení serveru	2	8	16
8	Špatná interpretace stavu zabezpečení	4	6	24
9	Ztráta důvěry následkem prolomení zabezpečení	3	8	24
10	Ztráta přístupu k serveru	2	7	14
11	Zašifrování dat ransomware útokem	3	9	27
12	Nedostatek prostoru pro detekci slabin	4	5	20
13	Odstavení serveru	2	9	18
14	Únik osobních údajů	3	9	27

Tabulka 4 Popis a ohodnocení hrozeb

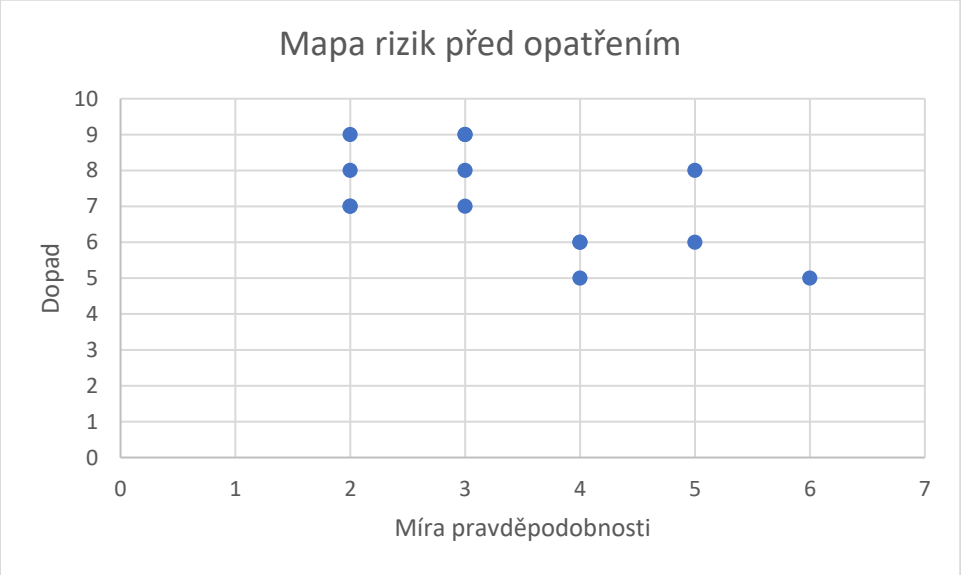
[Zdroj: vlastní zpracování]

Po vytvoření tabulky s popisem hrozeb je třeba vytyčit hrozby, které mají hodnotu nad určenou hranicí. Tuto hranici jsem určil na úrovni 30 a více, jelikož se jedná o středně závažné hrozby. Hrozbami nad touto hranicí jsou:

- Neschopnost detekce zranitelnosti (hodnota: 30)
- Neschopnost zabezpečení zranitelnosti (hodnota: 30)
- Využití zranitelnosti otevřeného portu (hodnota: 40)

Samozřejmě se nesmí zapomínat na ostatní hrozby, které se této hranici blíží, ale buď z pohledu pravděpodobnosti nebo dopadu nejsou pro projekt tak kritické.

V následujícím grafu je znázorněna mapa rizik jednotlivých hrozeb v závislosti na pravděpodobnosti a dopadu. Jelikož má více hrozeb stejné ohodnocení, může jeden bod označovat dvě hrozby.



Graf 1 Mapa rizik před opatřením

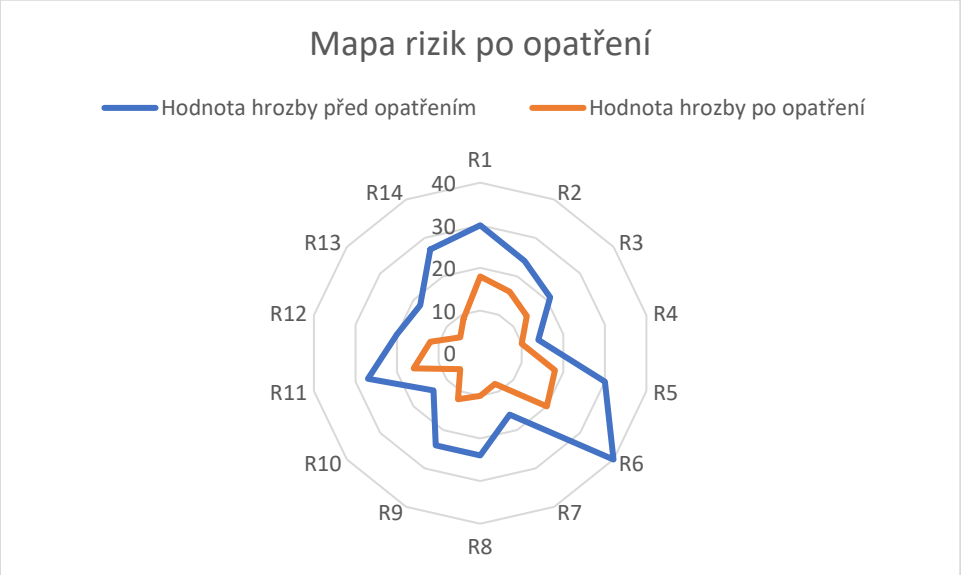
[Zdroj: vlastní zpracování]

V další části analýzy zpracuji tabulku, kde uvedu opatření proti jednotlivým hrozbám, které sníží míru pravděpodobnosti jejich výskytu, případně ji úplně eliminuje. V následující tabulce tyto informace uvedu a následně tato opatření vynesu do grafu, kde bude zřetelné, jak které opatření je účinné.

ID	Popis opatření	Hodnota hrozby před opatřením	Hodnota hrozby po opatření
1	Zavedení systému pro detekci zranitelností	30	18
2	Dokumentace otevřených portů a následné skenování	24	16
3	Zavedení automatických aktualizací systému	21	14
4	Zavedení evidence verzí jednotlivých služeb a jejich pravidelná kontrola	14	10
5	Vytvoření návodu pro zabezpečení jednotlivých zranitelností, pravidelné školení	30	18
6	Nalezení otevřeného portu a jeho následné zabezpečení	40	20
7	Dodržování doporučení NÚKIB	16	8
8	Vytvoření návodu pro dokumentaci stavu zabezpečení	24	10
9	Zabezpečení sítě, aby byla pravděpodobnost prolomení minimální	24	12
10	Zavedení remote shellu	14	6
11	Instalace bezpečnostního software	27	16
12	Detailní rozvržení úkolů jednotlivým osobám	20	12
13	Zajištění backup serveru, který by převzal roli	18	6
14	Zašifrování osobních údajů	27	9

Tabulka 5 Popis a ohodnocení hrozeb po zavedení opatření

[Zdroj: vlastní zpracování]



Graf 2 Mapa rizik po opatření

[Zdroj: vlastní zpracování]

2.3 ANALÝZA BEZPEČNOSTI JEDNOTLIVÝCH PORTŮ A SLUŽEB

V další části se budu zabývat analýzou bezpečnosti jednotlivých portů. Jelikož ke každé aplikaci či službě na serveru se přistupuje přes jednotlivé porty, jejich zabezpečení je nedílnou součástí celkové bezpečnosti serveru. Služby mají většinou vyhrazené výchozí porty a je třeba zkontrolovat, jestli nejsou otevřeny nezáměrně. Obecně platí, že porty, které nejsou využívány by měly být blokované. Je však možné, že po updatu systému se nějaký port otevře, proto je nutné kontrolu portů provádět v určitých intervalech a nezanedbávat ji.

2.3.1 Port 0

Port 0 nepoužívá žádná ze služeb a neměl by se využívat ani žádnou aplikací. Představuje totiž určité bezpečnostní riziko. I když se port 0 oficiálně nevyužívá, komunikace může být na tento port směřována a pokud se dostane až k cílovému zařízení, může dojít k jeho zahlcení, jelikož tuto komunikaci začne zpracovávat. Tento port se tedy využíval dříve k DDoS útokům. Ochranu proti těmto útokům začali poskytovat do jisté míry už poskytovatelé připojení a to tím, že komunikaci směřovanou na tento port automaticky zahazují.

2.3.2 Port 20,21

Tyto dva porty jsou využívány ke komunikaci FTP serveru s klientem. Komunikace není šifrovaná, co se týče přenosu dat i autentizace. Porty jsou z tohoto důvodu zneužívány a pokud není FTP server správně nastaven, může dojít k úniku informací, jelikož podporuje tzv. anonymní režim, ve kterém není za potřebí žádné přihlášení.

2.3.3 Port 22

Port 22 se používá pro vzdálený management přístup přes SSH protokol. Využívá se na všech systémech, ale v drtivé většině u linuxových systémů. I když je tento protokol považován obecně za bezpečný, vyžaduje řádné nastavení klíčů. Na rozdíl od telnet protokolu, který je předchůdcem právě SSH je komunikace šifrovaná. Pro přístup lze místo hesla použít i RSA klíč.

2.3.4 Port 23

Tento port je využíván pro Telnet. Jak již bylo uvedeno výše, telnet protokol je nezabezpečený a nevyužívá v komunikaci šifrování. Všechny data i hesla se posílají v plain textu, čehož může být zneužito například při MITM útoku, kdy útočník může vyčíst z paketů použitá hesla. Je také hojně zneužíván malwary.

2.3.5 Port 25

Port 25 je využíván SMTP protokolem, který slouží k emailové komunikaci. Pokud není dostatečně zabezpečen, mohou přes tento protokol útočníci zasílat podvržené emaily, případně spamy.

2.3.6 Port 53

Přes port 53 komunikují DNS servery. Používá se tedy pro překlad doménového jména na IP adresu. Pokud daný server neposkytuje DNS služby, ale má tento port otevřený, může dojít k DDoS útoku, případně k odstavení celého serveru.

2.3.7 Port 69

Pokud je na serveru nastaven TFTP server, využívá právě port 69 pro komunikaci s klientem. Protokol je využíván pro triviální přenos souborů. Primárně se používá pro stažení nebo upload bootovacích souborů například u switchů nebo routerů. Bezpečnostní riziko představuje. Protože zde není potřeba žádné ověření, tudíž kdokoliv má přístup k TFTP serveru si z něj může stáhnout jakákoliv data.

2.3.8 Port 123

Port 123 se využívá pro NTP protokol. Jedná se o protokol pro časovou synchronizaci více zařízení. Využívá se například i u switchů, routerů nebo ostatních aktivních prvků například pro zpřesnění logů. Informace, které může potencionální útočník vyčíst, pokud bude tento port otevřený jsou například uptime zařízení, čas nebo různé statistiky.

2.3.9 Port 139, 445

Port 139 využívá služba NETBIOS. Tuto službu poskytuje na svých systémech společnost Microsoft. Tato služba může konkrétně využívat protokol SMB, který slouží k procházení souborů, sdílení zařízení v síti apod. Starší verze protokolu SMB jsou velmi náchylné na útoky, jelikož obsahovaly mnoho chyb a zranitelností. Další typ útoku, který by mohl cílit na port 139 je jako u předešlých DDoS.

V roce 1996 Microsoft přesunul protokol SMB na port 445, aniž by musel používat službu NETBIOS. Přesun na tento port byl poprvé k vidění v systému Windows 2000. V současné době je využíván protokol SMBv3, kde je výrazně zlepšena právě bezpečnost a výkon. Protokol SMB byl využit v roce 2017 při velkém kybernetickém útoku WannaCry, který zasáhl několik set tisíc zařízení.

Služba NETBIOS běžně využívá port 139, ale pro jiné účely může použít i 137 a 138.

2.3.10 Port 389

Tento port využívá služba LDAP především v Active Directory ve Windows. Je to služba pro správu uživatelských účtů a přes port 389 probíhá autentizace zařízení i uživatele. Dále pak doménový kontroler předává koncovým zařízením informace o politikách.

V květnu roku 2020 byla zneužita chyba právě v autentizaci AD, kdy díky špatné implementaci kryptografického šifrování bylo možné odstranit heslo z účtu SERVICE a spustit si tak administrátorský powershell.

2.3.11 Port 1433, 1434, 3306

Tyto porty jsou používány databázovými programy, konkrétně MS SQL nebo MySQL servery. Používají se například pro komunikaci mezi databází a webovou stránkou nebo nějakou aplikací. Pokud nejsou zabezpečeny, může přijít DDoS útok, popřípadě se tyto porty využívají při malwarové distribuci.

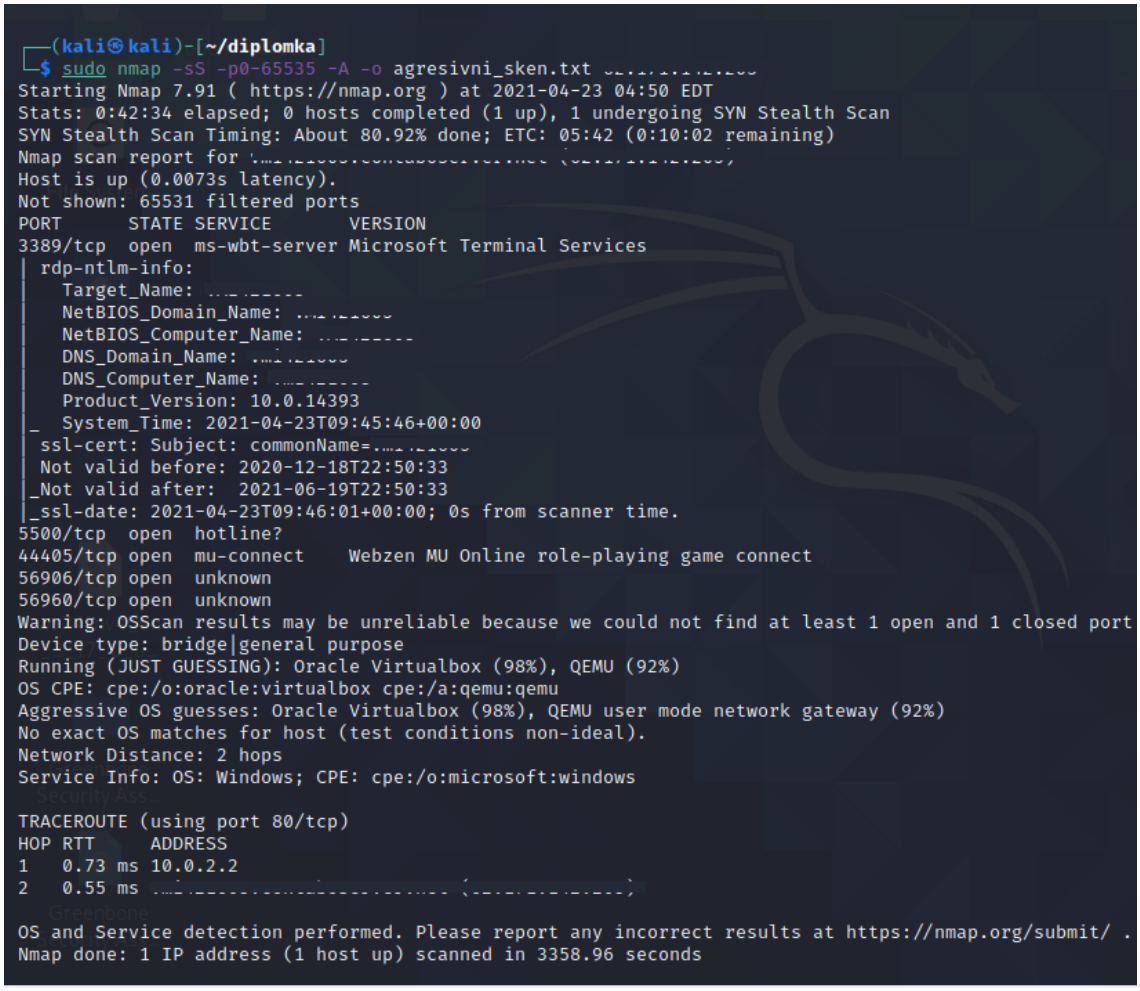
2.3.12 Port 3389

Jedná se o port využívaný při připojení vzdálené plochy. Služba využívá RDP protokol. Tento protokol je jedním z nejzranitelnějších na platformě Windows a také je díky tomu hojně využívaný. Bylo nalezeno již několik exploitů, které využívalo právě zranitelnosti RDP. Nejznámější zranitelností je Bluekeep, kdy se do paměti zařízení nahrál infikovaný kód, který umožnil útočníkovi převzít kontrolu nad zařízením.

2.4 Analýza bezpečnosti za použití nástrojů

Tato část diplomové práce je spíše prakticky zaměřená. Za pomocí nástrojů oskenuji server, zda má otevřené nějaké porty, popřípadě které a jestli na těchto portech běží služby, které jsou nějakým způsobem zranitelné.

Z každého nástroje uvedu výsledky ve formě obrázku. Pro bezpečnost serveru na obrázcích nebude vedena IP adresa a název počítače v síti poskytovatele. Jako první nástroj pro skenování serveru jsem využil nástroj nmap. Pro testování využívám operační systém Linux, konkrétně distribuci kali, která je určena k penetračním testům a má nástroje pro tyto účely nainstalovány už ve výchozím nastavení. Je důležité říct, že tyto nástroje můžou obsahovat chyby, a proto je dobré použít pro skenování nástrojů více.



Obrázek 7 Nmap sken serveru

[Zdroj: vlastní zpracování]

Při skenování pomocí nástroje nmap jsem použil příkaz „sudo nmap -sS -p0-65535 -A -o agresivní_sken.txt XXX.XXX.XXX.XXX“. Sudo je příkaz pro práci v administrátorském režimu, který je nutný, pokud se provádí určité typy skenů. Argument -sS říká, že nástroj bude provádět sken pomocí TCP SYN paketů, -p0-65535 je parametr pro skenování všech portů serveru, bez tohoto argumentu by nástroj oskenoval pouze ty, které jsou nejvíce používaný v běžných systémech. Argument -A říká, že se jedná o agresivní sken, součástí kterého je pokus o zjištění operačního systému, jaké služby běží na portech apod. Pokud se nastaví ale agresivní sken, většina bezpečnostních softwarů ho rozpozná a zablokuje. Z obrázku můžeme vidět, že prvním otevřeným portem, který nmap našel je port 3389. Ten je, jak jsem již zmiňoval, určen

pro RDP protokol. Jelikož je zde verze Microsoft Terminal Services, můžu předpokládat, že se jedná o zařízení se systémem od společnosti Microsoft.

Dalším otevřeným portem je 5500, který slouží jako autoupdater pro aplikaci klientů. Tuto informaci by však potencionální útočník přes nástroj nmap nezjistil.

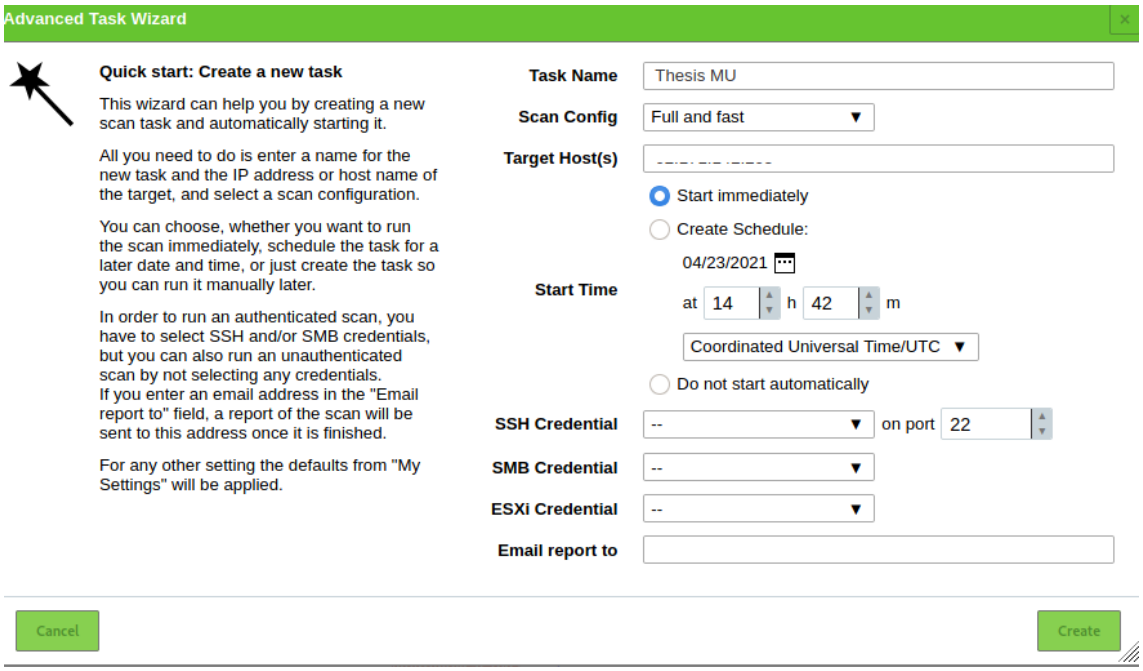
U portu 44405 už ale službu zjistit lze, tento port se využívá právě k připojení hráčů k aplikaci herního serveru.

Dalšími otevřenými porty jsou 56906 a 56960. Ty slouží stejně jako port 44405 při připojení hráčů k různým aplikacím pro korektní běh serveru.

Další věcí, na kterou se zde dá zaměřit je popis operačního systému. Ze služby na portu 3389 je zřejmé, že se jedná o systém Windows, avšak nmap říká, že se na 98% jedná o systém Oracle Virtualbox. Z těchto informací lze říci, že server bude virtualizovaný právě se systémem Windows.

Posledním ukazatelem zde je nástroj trace route, který ověří, kolik hopů je server vzdálen od zařízení provádějící sken. Z obrázku však lze říct, že se jedná o chybnou informaci, jelikož by se server musel nacházet hned za routerem.

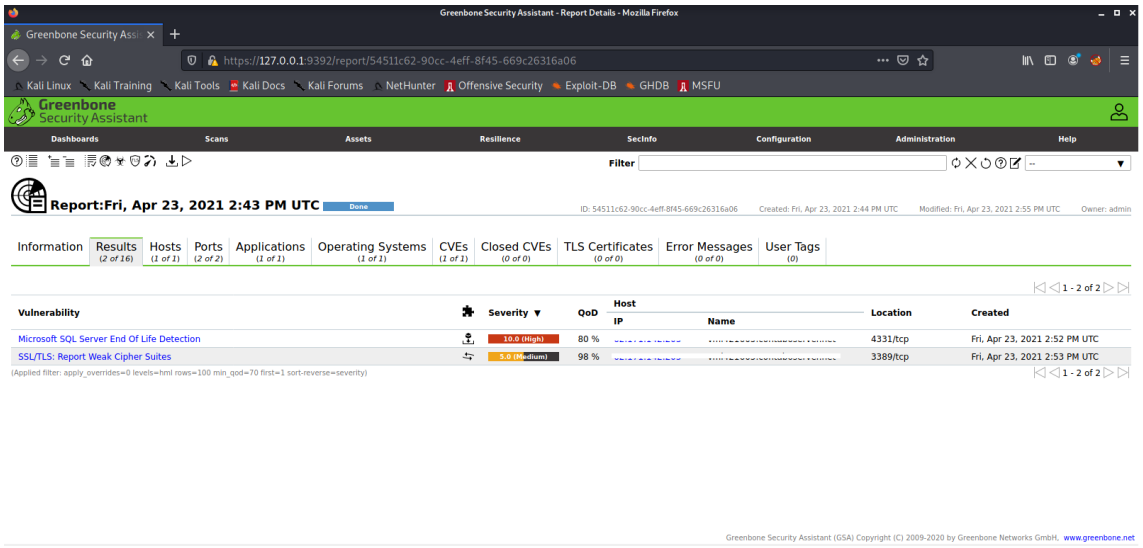
Dalším nástrojem, který jsem využil pro skenování chyb je open-vas. Jedná se o nástroj, který má grafické rozhraní na rozdíl od nmap a zobrazuje zároveň zranitelnosti, které mohou být pří potencionálním útoku využity. Výhodou tohoto nástroje je také možnost nastavit si uživatelské údaje pro SSH, SMB nebo ESXi, které by mohly být využívány na cílovém serveru. Je zde jako u nmapu několik typů skenu. Pro tuto práci jsem zvolil sken „Full and fast“, který je pro mé účely dostačující. V následujícím obrázku je task wizard nástroje open-vas. Nástroj je pro běžné testování jednoduchý na správu.



Obrázek 8 Task wizard u nástroje open-vas

[Zdroj: vlastní zpracování]

V následujícím obrázku jsou již výsledky skenu.



Obrázek 9 Výsledky open-vas skenu

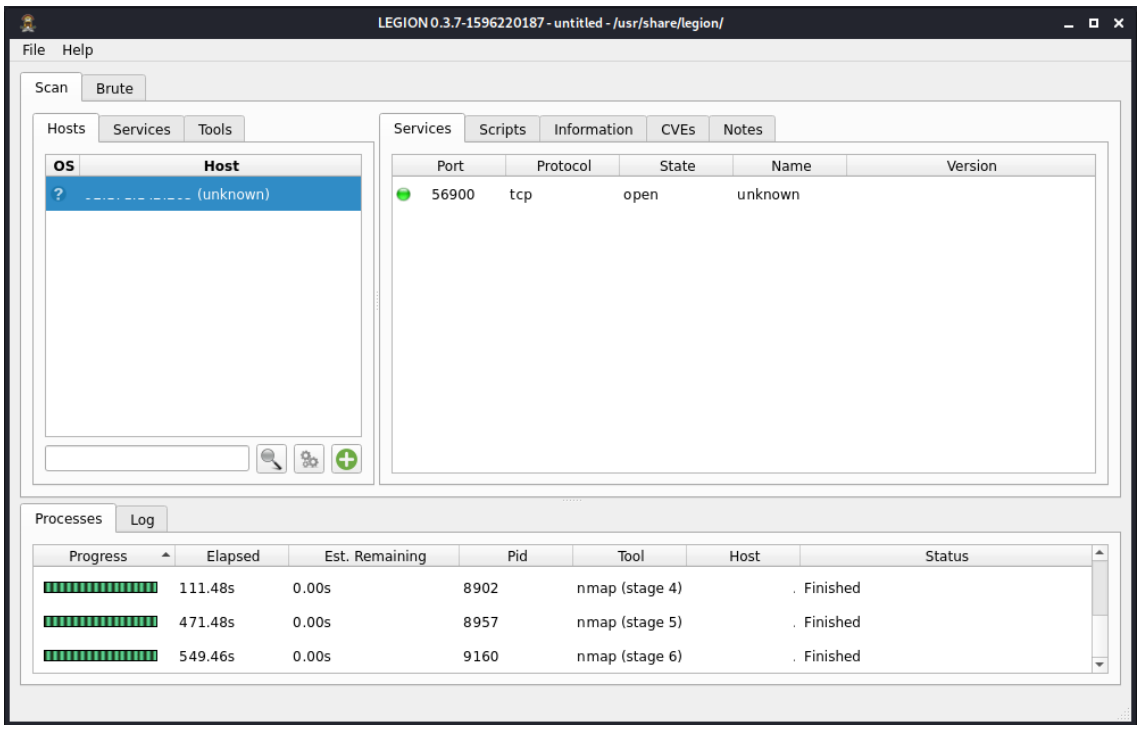
[Zdroj: vlastní zpracování]

Z obrázku je patrné, že server má jednu zranitelnost, která je ohodnocena hodnotou 10 jako kritická a jednu zranitelnost ohodnocenu hodnotou 5 čili medium.

Kritická zranitelnost je na TCP portu 4331, kde běží MS SQL. Podle reportu se jedná o aplikaci MSSQL 2008 R2, na kterou již Microsoft nevydává podporu, a tudíž je velmi nebezpečné ji stále používat, jelikož se můžou objevit zranitelnosti, na které již nebudou updaty.

Další zranitelností je slabé šifrování v protokolu RDP na portu 3389. Tato zranitelnost může být zneužita pro získání dat z přenosu přes port 3389. U těchto dat je možnost, že by je potencionální útočník mohl rozšifrovat a získat k nim přístup.

Třetím nástrojem, který jsem využil pro skenování je Legion. Tento nástroj je také implementován ve výchozím nastavení kali linuxu. Legion dokáže pracovat a sdružovat více nástrojů dohromady. V tomto testu byl použit nástroj nikto a znovu nmap, Legion s nmapem pracuje v rámci jiných argumentů, proto bylo možné, že se výsledky budou lišit.



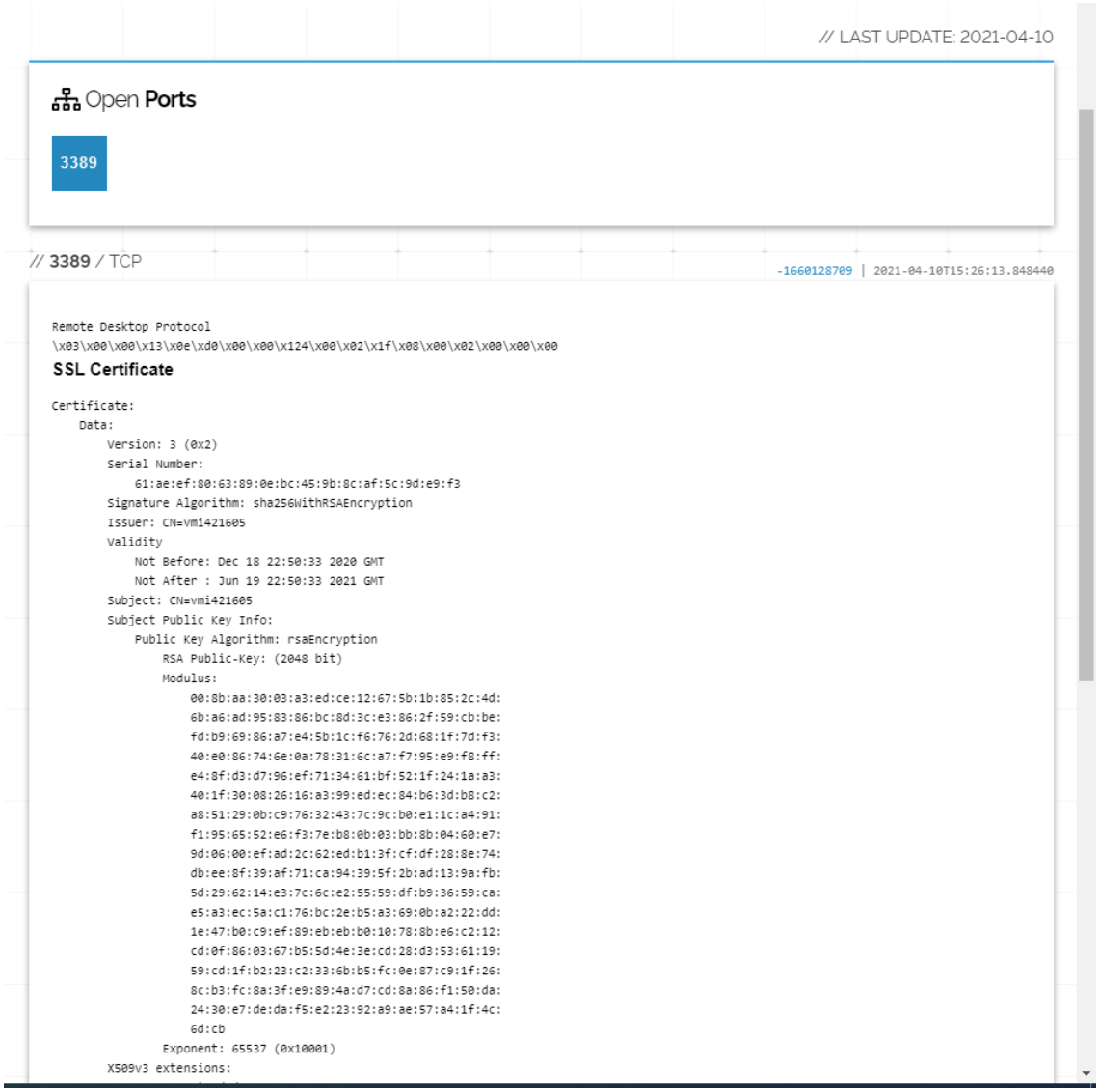
Obrázek 10 Report z nástroje Legion

[Zdroj: vlastní zpracování]

Nástroj Legion mi toho řekl o serveru v podstatě nejméně, pouze, že je otevřený port 56900. Jak jsem již ale uváděl, při testech je dobré prozkoušet více nástrojů, jelikož se

výsledky mohou lišit a dá se přijít na chyby, na které by se při použití jiného nástroje nepřišlo.

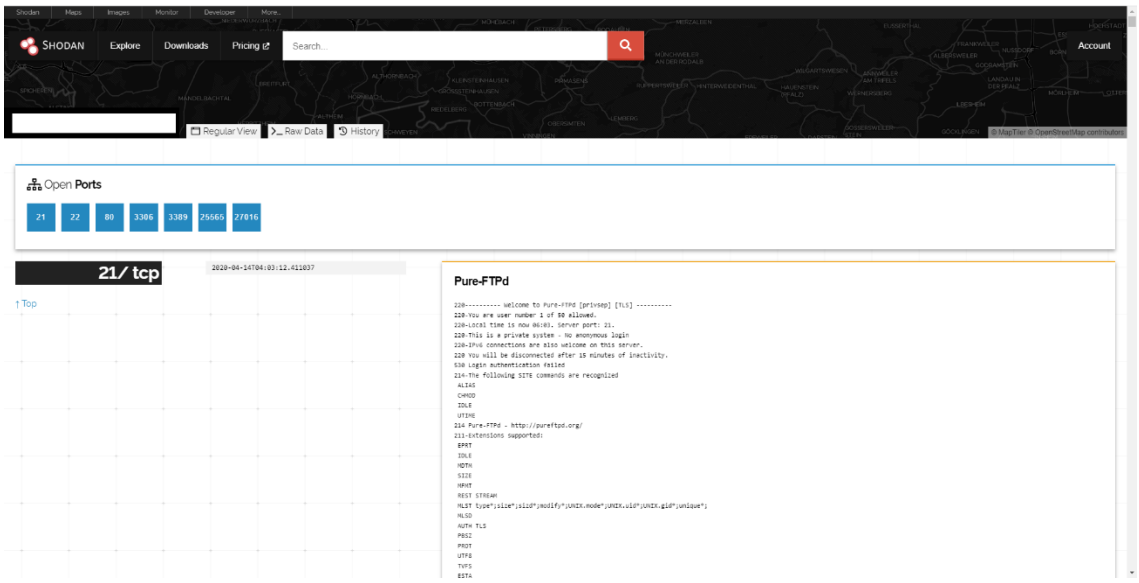
Posledním nástrojem, který jsem použil byl shodan.io, který v určitých časových intervalech monitoruje všechny dostupné IP adresy na světě a poskytuje o nich informace. Shodan.io nezkoumá všechny otevřené porty, ale pouze ty, které jsou nejvíce využívané. Na dalším obrázku lze vidět otevřený port 3389.



Obrázek 11 Skenování za pomoci Shodan.io

[Zdroj: vlastní zpracování]

Tyto informace uchovává i historicky s přesným datem, kdy byly pořízeny. Lze tedy procházet postupnou historii zabezpečení. Informace obsahují verze služby, která na daných portech běžela a uchovávají se zde více než rok.



Obrázek 12 Historie otevřených portů na serveru

[Zdroj: vlastní zpracování]

Na obrázku můžeme vidět, že v minulosti bylo na serveru otevřeno mnohem více portů než v současnosti, což mohlo vést se špatným zabezpečením ke kompromitaci. Například u portu 21 můžeme vidět, že byl otevřený naposledy při skenování, které shodan provedl 14.4. roku 2020 a běžela na něm služba FTP. Nástroj zkouší předem definovaný login a zároveň, jestli je dostupný Anonymous login, který jak jsem popisoval výše může být zneužit útočníkem.

Dalším příkladem je port 80, který byl na serveru otevřený chvíli z důvodu provozu http serveru přes službu apache. Tato služba byla na serveru spuštěna z důvodu testování webových stránek, které k serveru náleží. Později byly stránky přesunuty na vlastní web hosting.

Shodan.io je komplexní nástroj a poskytuje mnoho funkcí, které se dají použít nejen při nárazovém testování, ale i při udržování analýzy serveru. Této funkci se budu věnovat v návrhu řešení.

Závěrem bych chtěl dodat, že agresivní skenování, které jsem použil v nmapu, popřípadě full skeny v open-vas apod. se legálně nesmí provádět na zařízeních, u kterých to není povoleno majitelem.

3 VLASTNÍ NÁVRHY ŘEŠENÍ

V této části diplomové práce popisuji vlastní návrh řešení. To obsahuje odstranění zranitelností serveru, které byly odhaleny v minulé části, ale také zabezpečení z pohledu aplikací a monitorování serveru. Návrh je směřován i pro budoucí kroky projektu, tudíž vezmu v potaz i DNS server a DHCP server, které by mohly být v budoucnu využívány. Všechna navrhnutá řešení budou postupně na server aplikována.

3.1 SERVEROVÉ ŘEŠENÍ

V první řadě je potřeba určit, jaké nároky budou potřeba na server. Na server se připojují lidé z důvodu hraní hostované hry. Hra může běžet pouze na Windows zařízeních, tudíž je třeba vzít v potaz systém, jaké služby na něm poběží a určit, kolik hráčů se zhruba na server bude připojovat, aby nedocházelo poklesu latence u klienta.

Na serveru poběží také monitorovací systém, který zjišťuje počet připojení z jedné IP adresy a dále vyhodnocuje podle zadaných parametrů, zda je připojení v pořádku, nebo z dané IP adresy probíhá nějaký typ útoku. DHCP server, který bude nastaven a zabezpečen pro budoucí účely společně s DNS serverem. Na serveru také poběží Active Directory, aby mohli ostatní lidé v týmu pracovat se serverem, měli přístup k souborům, které tam jsou uloženy, případně si pak účty propojit s emailovými adresami.

3.1.1 Hardwarové požadavky

Pro všechny výše zmiňované služby bude třeba server s alespoň se čtyřmi jádry a 16GB RAM paměti. Vyšší operační paměť je z toho důvodu, že na serveru běží 3 herní sub servery, pro lepší zážitek hráčů. Další hlavní komponentou je HDD, jelikož se každý den zaznamenávají logy a zaznamenává se každá akce jednotlivých hráčů, logy zabírají až 1,5GB místa za jeden den. Dále se každou hodinu zálohuje databáze, u které každá záloha zabere minimálně 100MB. Pro uchování alespoň měsíce logů, databáze a dalších věcí je tedy třeba alespoň 500GB velký HDD. Server může být prozatím virtuální, do budoucna je ale v plánu, že se přesune na dedikovaný pro lepší manipulaci. Posledním požadavkem je připojení k síti a bandwith, pro hladký chod serveru stačí 100Mb/s download i upload.

Jelikož hráči mají klientské soubory na svých počítačích a server se dotazují pouze na několik informací, více není potřeba.

3.1.2 Softwarové požadavky

Jak jsem již zmiňoval, hru je nutné provozovat na operačním systému Windows. Nejlépe samozřejmě na nejnovější serverové verzi, což je v této době Windows Server 2019. Není však nutná edice datacenter, ale stačí standard. Dalším softwarem, bez kterého by provoz serveru nebyl možný je Microsoft SQL server. Jak bylo uvedeno v analytické části, nyní server využívá MS SQL 2008 R2, který již není společností Microsoft podporovaný, a tudíž bude třeba se bude třeba na tuto skutečnost zaměřit. Nesmí zde také chybět samozřejmě serverové soubory hry MU online, přes které se celý herní svět nastavuje a na které se hráči připojují. Soubory jsou naprogramovány v jazyku C#. Dalším požadavkem je monitorovací systém od společnosti SolarWind. Další složkou je automatický update server, který slouží hráčům ke stažení aktualizací. Po zapnutí hry se automaticky klient dotáže na update server, zda má poslední verzi a pokud ne, verze se mu stáhne a následně nainstaluje. Poslední složkou je program podobný linuxových cron jobům, který má za úkol automatické zálohování databáze.

3.2 POŽADAVKY NA PRACOVNÍ STANICE V TÝMU

Abychom v týmu mohli provádět testování bezpečnosti, je třeba, aby měl každý člen pracovní stanici, která bude schopná toto testování provádět. Je rozdíl, zda se provádí například testy otevřených portů a služeb, které jsem provedl v analytické části této práce nebo simulace brute force útoků na RDP či databázi. Aby se členové týmu dostali do hry, potřebují také zařízení se systémem Windows, pro testy je ale lepší zařízení s linuxovým jádrem, konkrétněji například kali linux. Samozřejmě na testy není nutné mít dvě rozdílné zařízení, stáčí si spustit systém s linuxovým jádrem z virtuálního prostředí. Docílit se toho dá pomocí aplikace Virtual box nebo VM ware. Pro tyto zařízení jsou dostačující 2-4 jádra procesoru a alespoň 8GB RAM.

Pro brute force útoky je vhodná výkonnější grafická karta, jelikož se při tomto procesu snaží buď uhádnout heslo za pomocí určitých parametrů. Tento proces těží z výpočetního výkonu grafické karty a je také mnohem rychlejší. Platí také, že je zde lepší mít spuštěný

přímo systém na linuxovém jádru a nespouštět ho z virtuálního prostředí. Může se stát, že si virtualizace dokonale neporadí s ovladači, případně celkově s grafickým čipem a výpočetní výkon karty nebude plnohodnotný. Brute force útoky se rozumí buď uhádnutí přihlašovacích údajů za pomoci určitých parametrů nebo rozhashování zašifrovaných údajů. Pro tyto testy jsou teda vhodné zařízení s grafickou kartou, která má co nejvyšší hash rate. Ostatní komponenty mohou být stejné jako u testu portů.

3.3 ZABEZPEČENÍ SLUŽEB

Před spuštěním jakékoliv herního projektu je třeba zabezpečit služby, některé se dají zabezpečit přidáním pravidla do Windows firewallu, některé z konfiguračních složek a některé přímo z registrů. Některé služby, případně porty nelze ale zakázat úplně, jelikož by byla kompletně znepřístupněna komunikace i členům týmu, u kterých to nemusí být žádoucí.

3.3.1 Přemostění portů

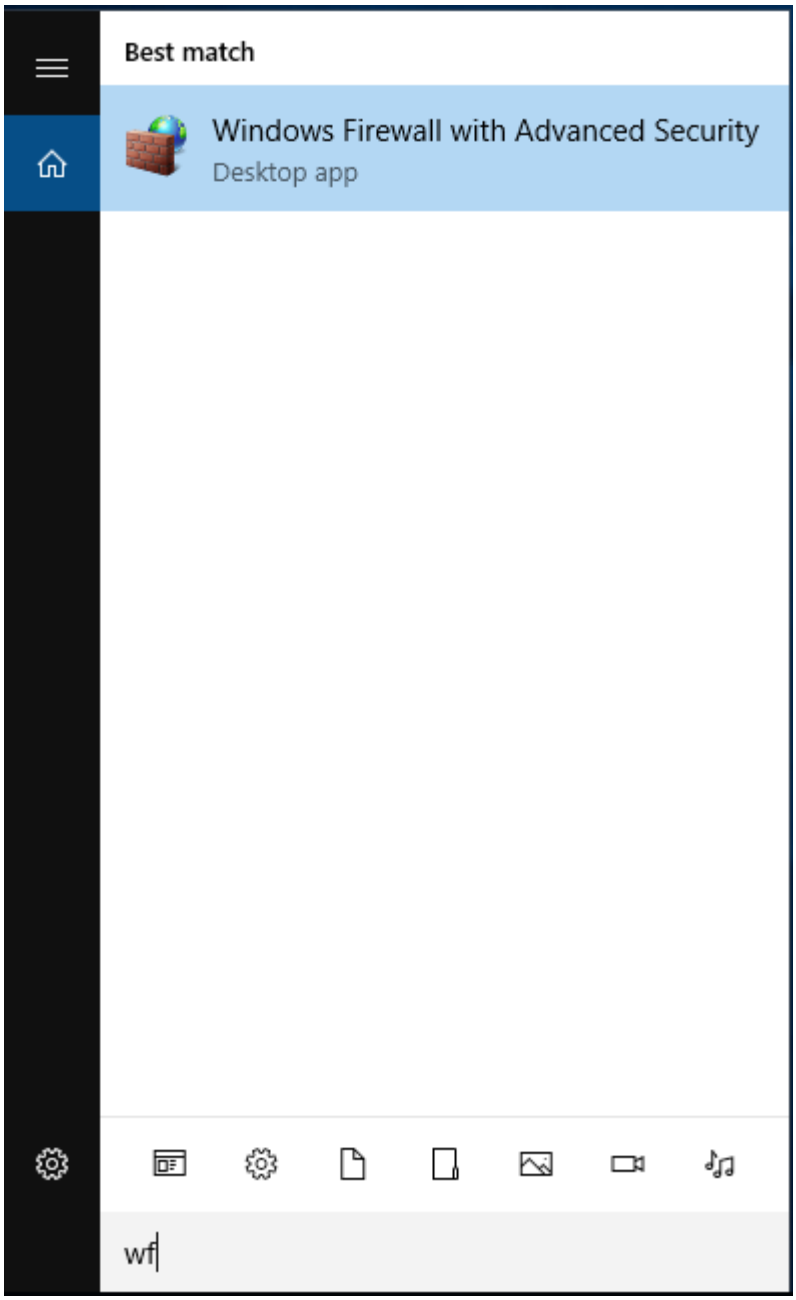
V síti internetu je dnes mnoho botů, kteří ověřují všechny veřejné IP adresy, které jsou připojeny do internetu. Tyto adresy potom zkoumají a pokud mají otevřené určité porty, mohou se přes ně snažit zařízení kompromitovat. Dvěma z hlavních takto zneužívaných portů jsou 1433 a 3389. První z portů 1433 byl používán přímo na herním serveru pro komunikaci s MS SQL serverem a chvíli po spuštění na tento port cílily útoky v rámci statisíců dotazů týdně. Útok byl cílený na prolomení přihlašovacích údajů výchozího administrátorského účtu „sa“. Prvním krokem tedy bylo vytvořit nový administrátorský účet, deaktivovat účet „sa“ a přemostit databázi, aby poslouchala na jiném portu. Toto opatření rapidně snížilo počet pokusů o přihlášení. Stejně tak to platí pro port 3389, kde pouze přemostění komunikace RDP na jiný port znamenalo velký pokles pokusů o přihlášení.

3.3.2 Firewall pravidla

Primárně se věnuji zabezpečení pomocí firewallových pravidel. Je potřeba si určit, které porty jsou potřeba nechat otevřené, které můžu naopak zavřít a ke kterým by měl mít

přístup pouze autorizovaný člověk. Tato pravidla můžeme přidávat, odebírat čí upravovat následujícím způsobem:

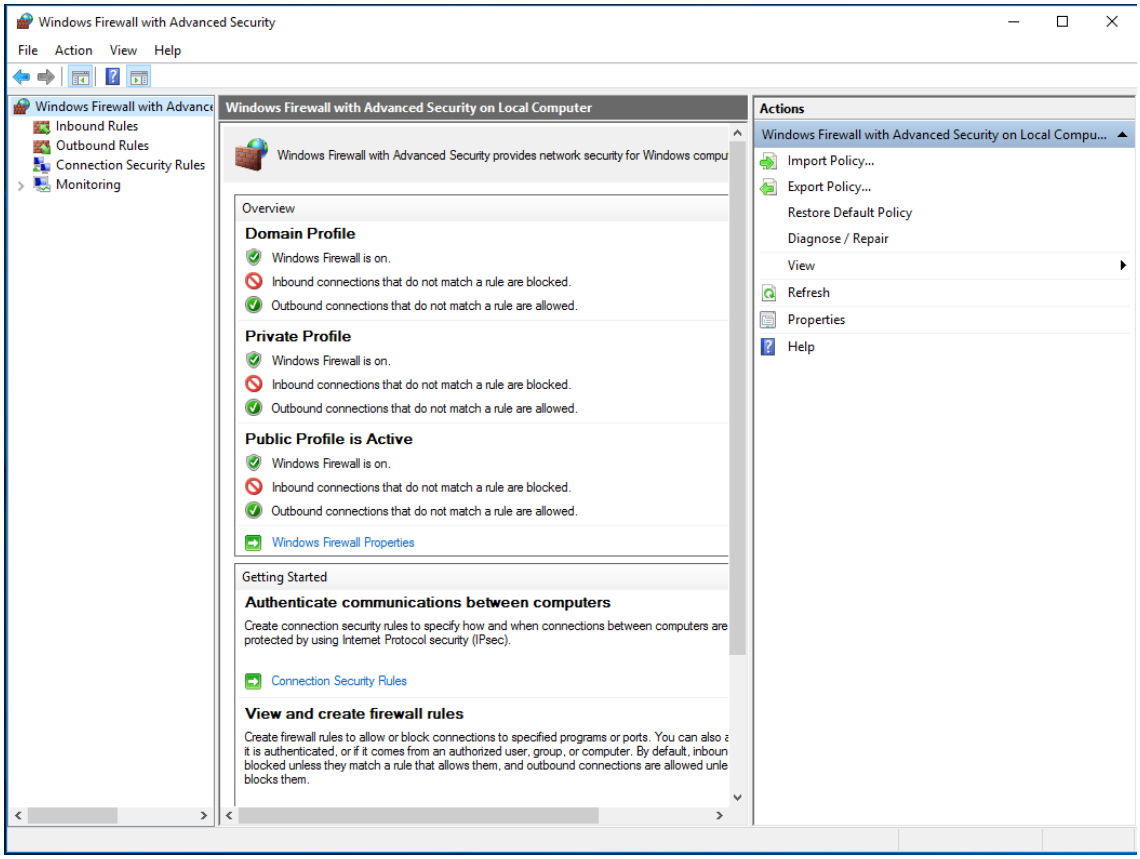
Jako první se musí spustit Windows Firewall s rozšířenými možnostmi, který najdeme ve vyhledávacím okně pod zkratkou „wf“



Obrázek 13 Vyhledání Windows firewall

[Zdroj: vlastní zpracování]

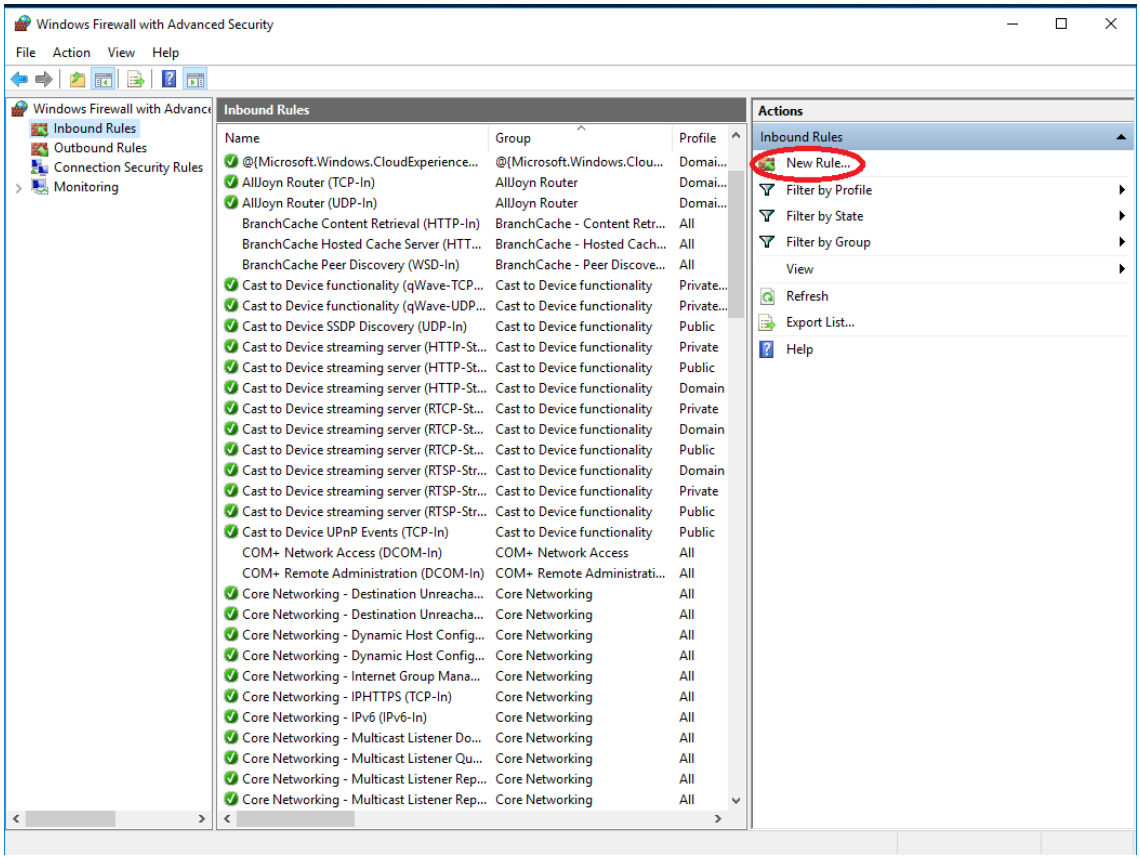
Po spuštění lze vidět, v jakém profilu je možné pravidla přidávat či upravovat. Dále lze v levém menu vybrat, zda se bude jednat o příchozí pravidlo nebo odchozí. Rozdíl spočívá v tom, že u příchozích pravidel se povolují porty a aplikace, na které uvidí klienti. Odchozí pravidlo se používá například u DHCP serveru, kdy server přiřazuje určitému zařízení IP adresu.



Obrázek 14 Počáteční rozhraní Windows firewallu

[Zdroj: vlastní zpracování]

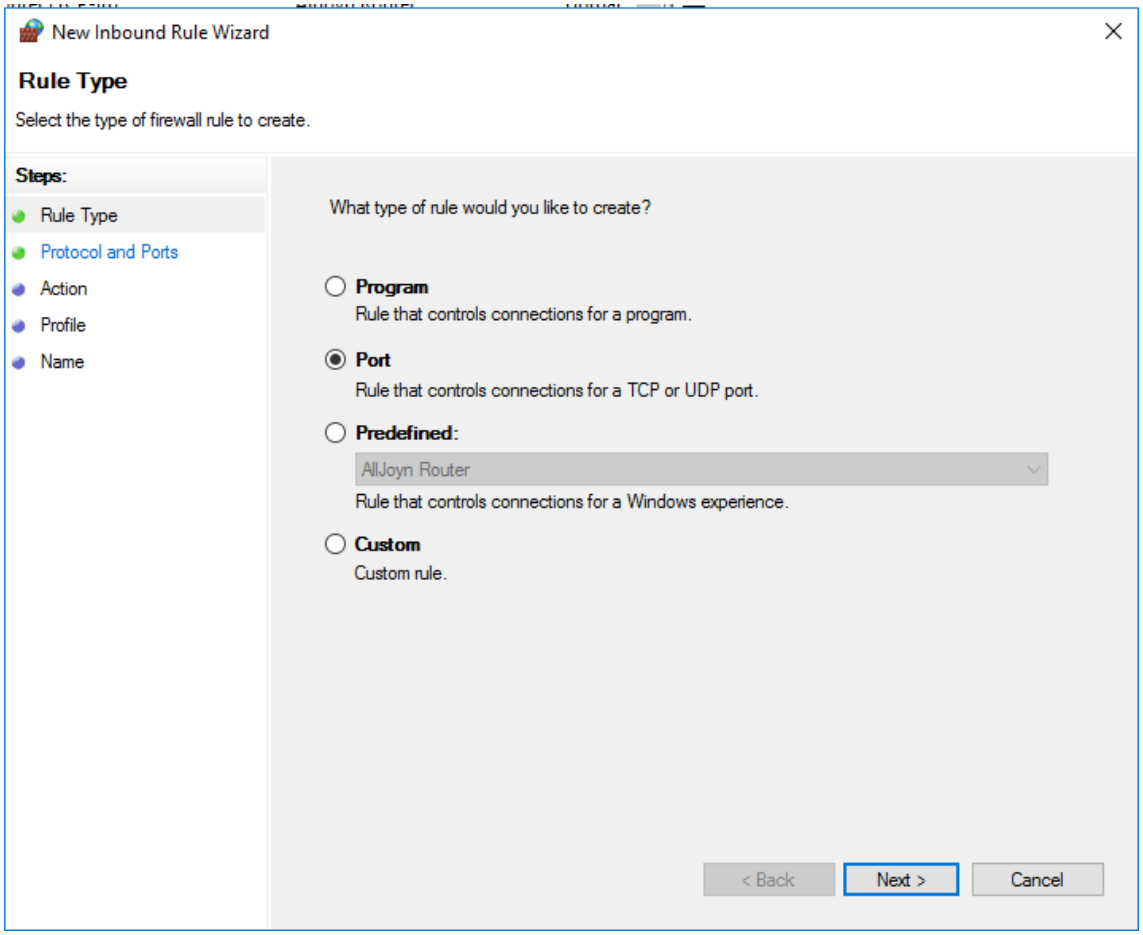
Na serveru je nutné nastavit hlavně příchozí pravidla. Ty se dají nastavit přes tlačítko „New rule…“ v záložce Inbound Rules.



Obrázek 15 Inbound pravidla a jejich přidání

[Zdroj: vlastní zpracování]

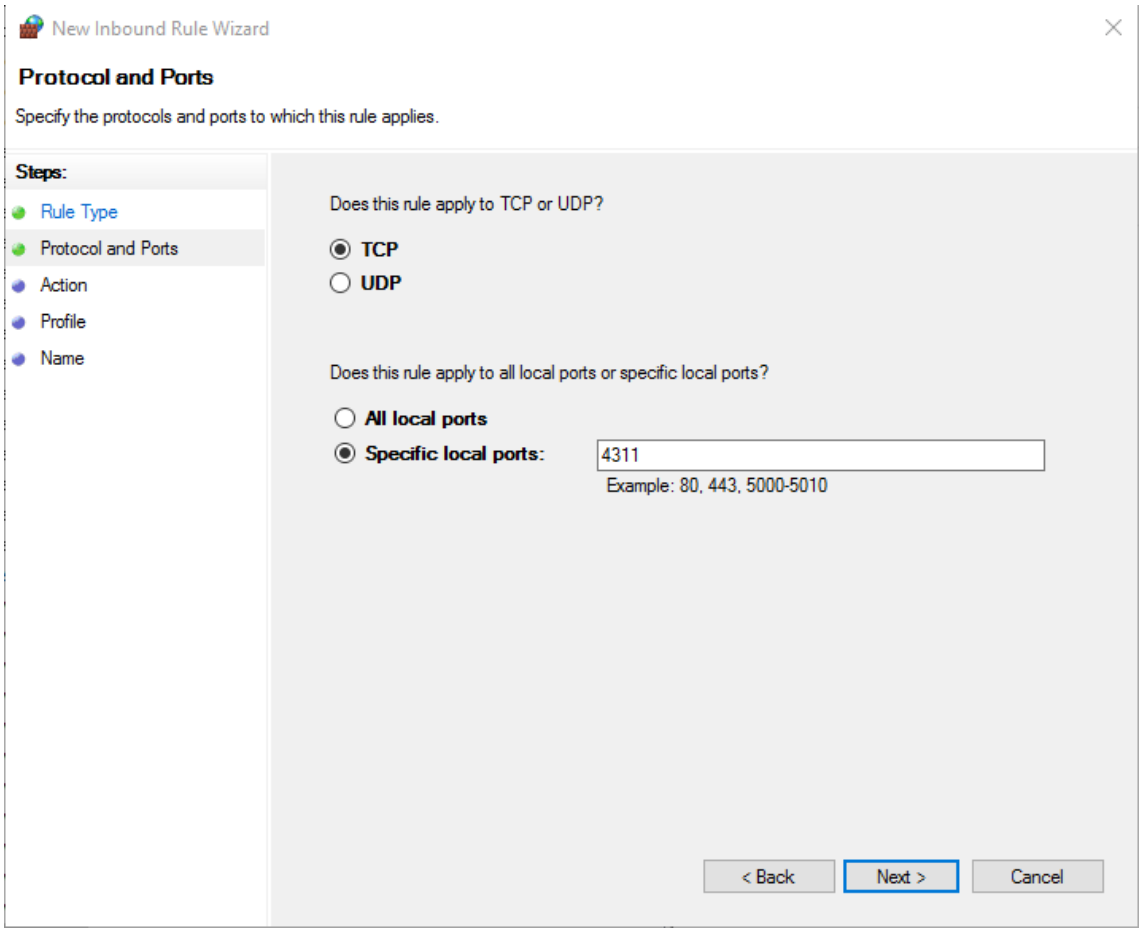
Po otevření okna lze vybrat, jaké pravidlo chceme přidat, může se jednat o pravidlo pro program, port, předdefinované pravidlo nebo si nastavit vlastní pravidlo. Pro účely této práce a celkově projektu stačí určit pravidla pro určité porty.



Obrázek 16 Výběr typu pravidla

[Zdroj: vlastní zpracování]

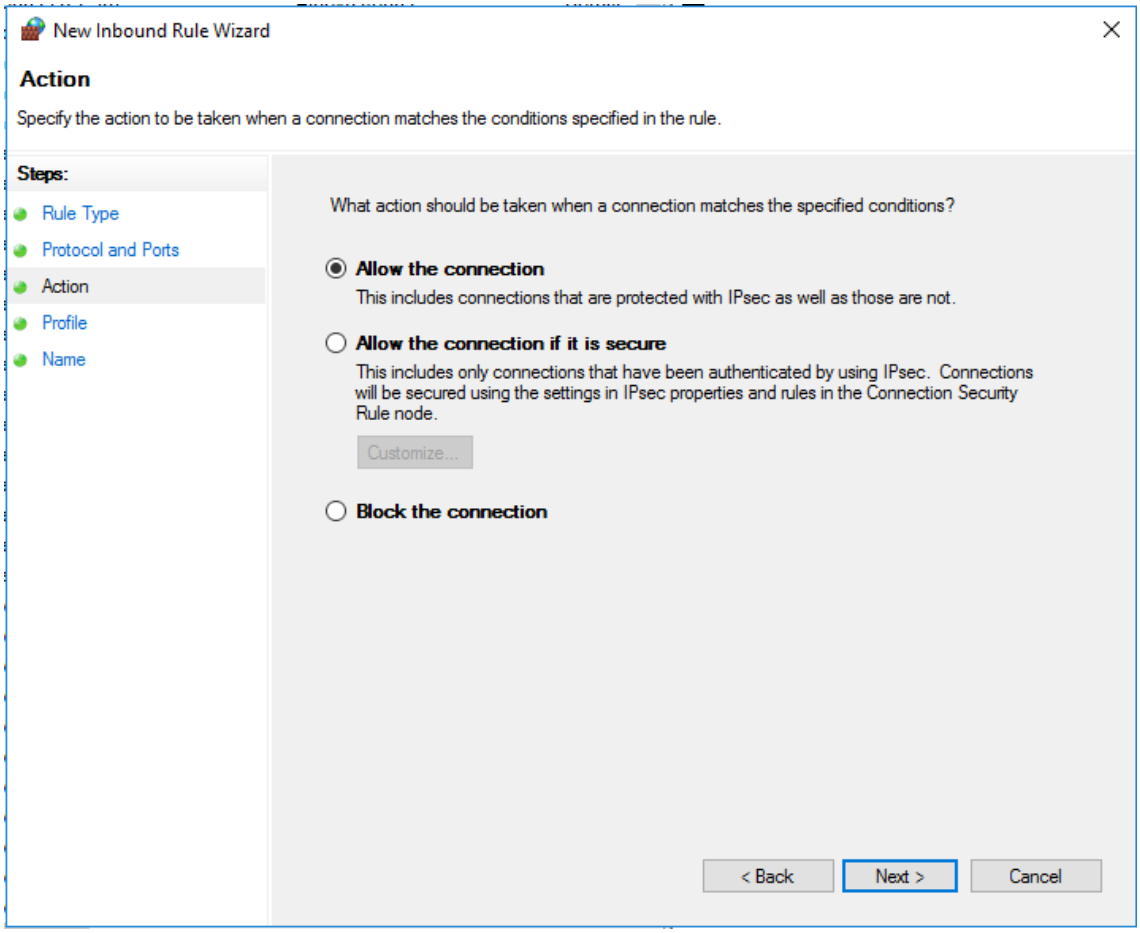
V dalším kroku je nutné specifikovat, zda se jedná o TCP port nebo UDP a určit, pro jaké porty toto pravidlo bude platit. V následujícím obrázku je zobrazen port 4311. Je to port, na který byla přemostěna komunikace s databázovým serverem.



Obrázek 17 Určení protokolu a portu pravidla

[Zdroj: vlastní zpracování]

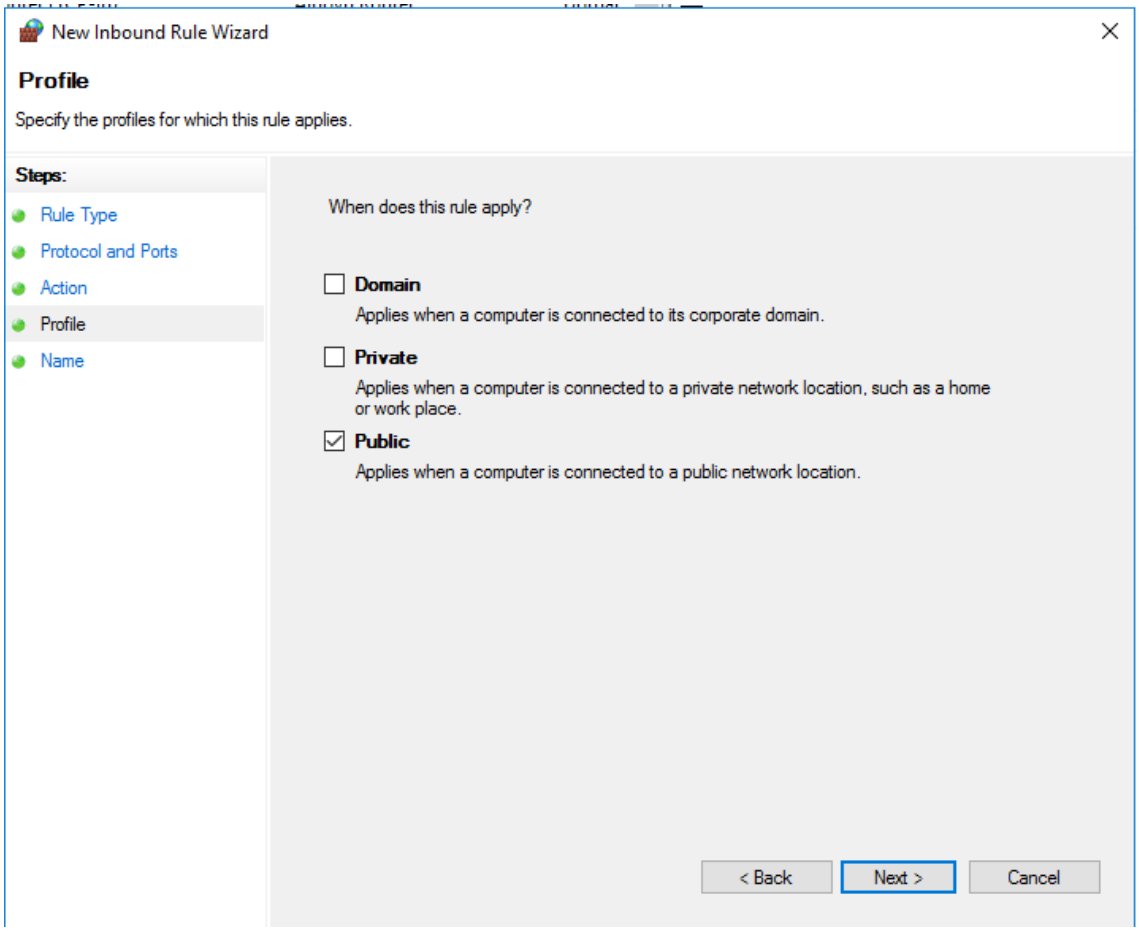
V další části je specifikace, jestli má být komunikace na daném portu povolena nebo se má blokovat. Pro účely projektu je nutné povolit připojení k portu.



Obrázek 18 Povolení připojení k portu

[Zdroj: vlastní zpracování]

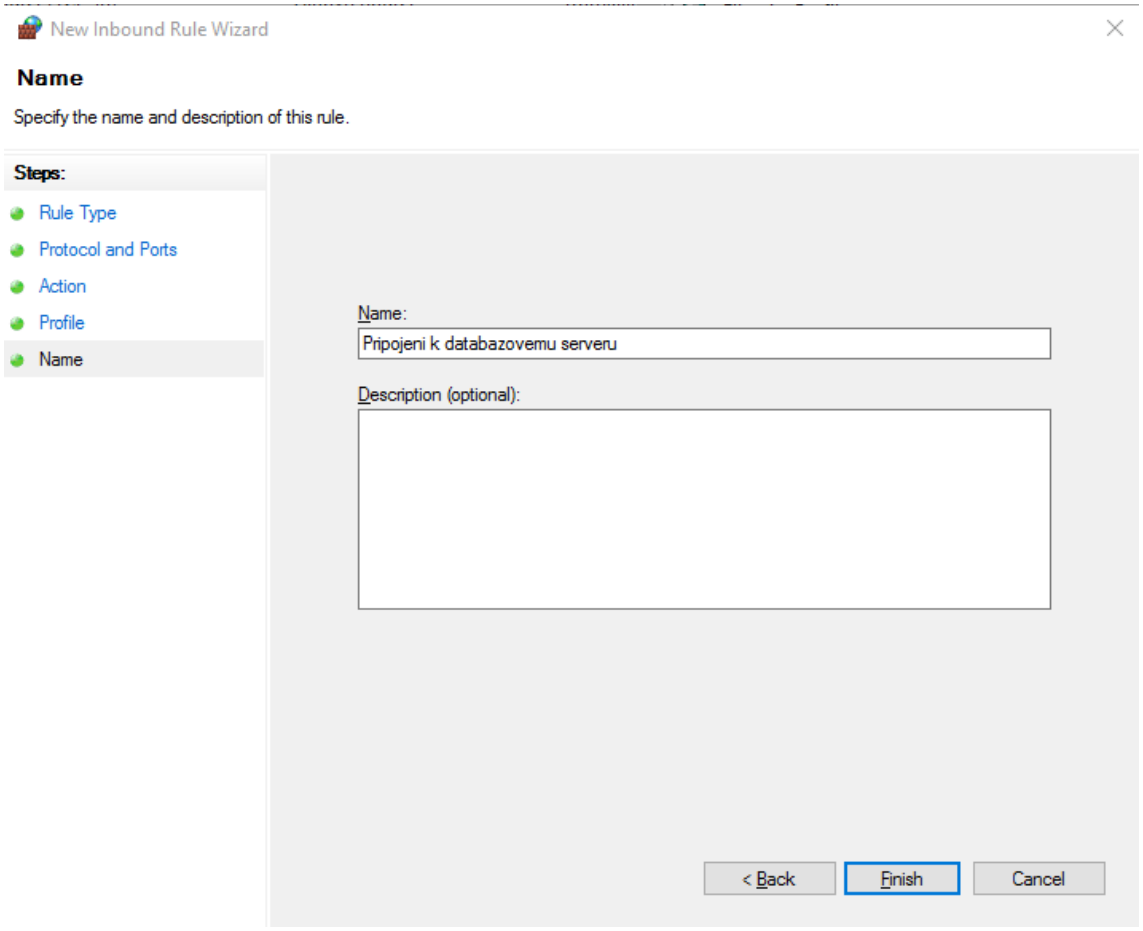
Jelikož je prozatím server hostovaný v Německu a nemáme jej v doméně, je třeba povolit připojení veřejné síti, což otvírá připojení do internetu.



Obrázek 19 Specifikace profilu připojení

[Zdroj: vlastní zpracování]

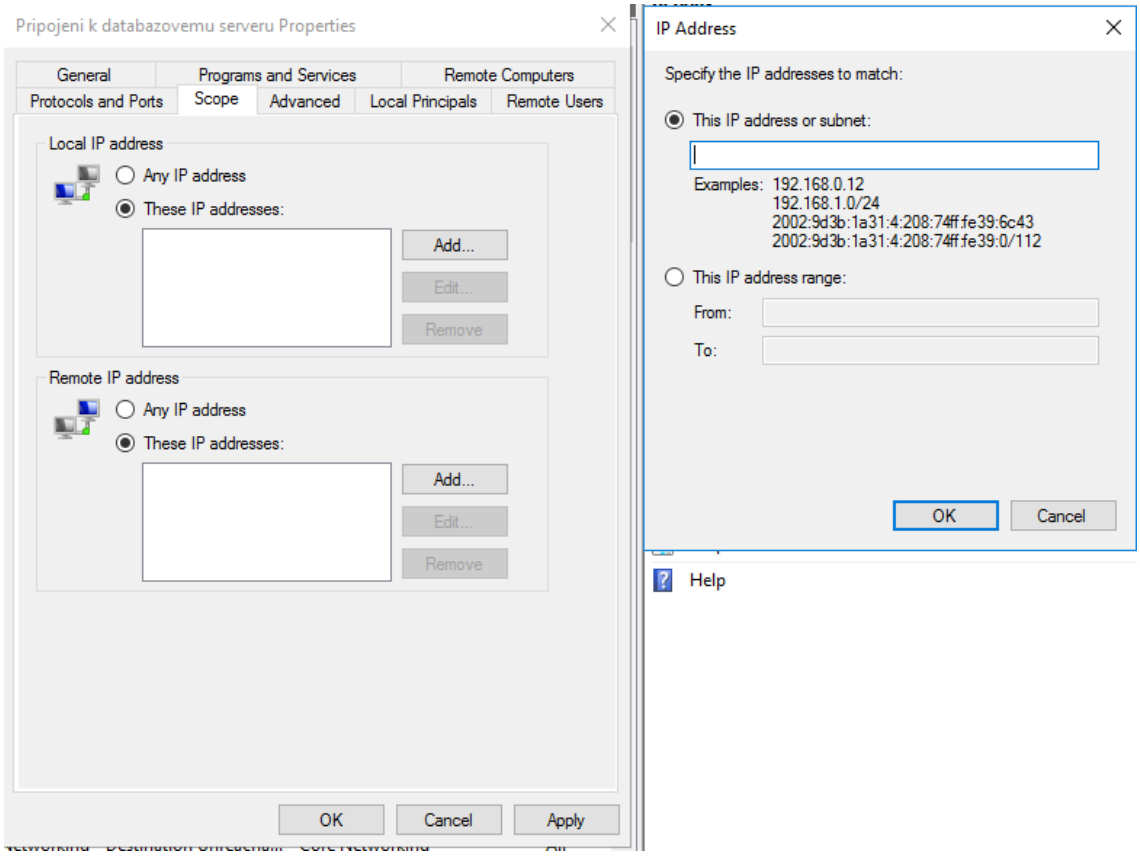
V posledním kroku je za potřebí určit název pravidla, popřípadě ho popsat pro lepší orientaci v pravidlech.



Obrázek 20 Pojmenování pravidla

[Zdroj: vlastní zpracování]

Potom přes záložku scope v možnostech daného pravidla lze určit, pro které IP adresy toto povolení bude platit. Jelikož se jedná o připojení do databáze, které vyžaduje program určený pouze členům týmu, nastaví se zde adresa každého člena týmu, případně bude potřeba VPN připojení s pevně danou IP adresou. IP adresy je třeba přidávat do skupiny Remote IP address, kde lze zadat IP adresy jednotlivě, případně z určitého rozmezí nebo subnety.



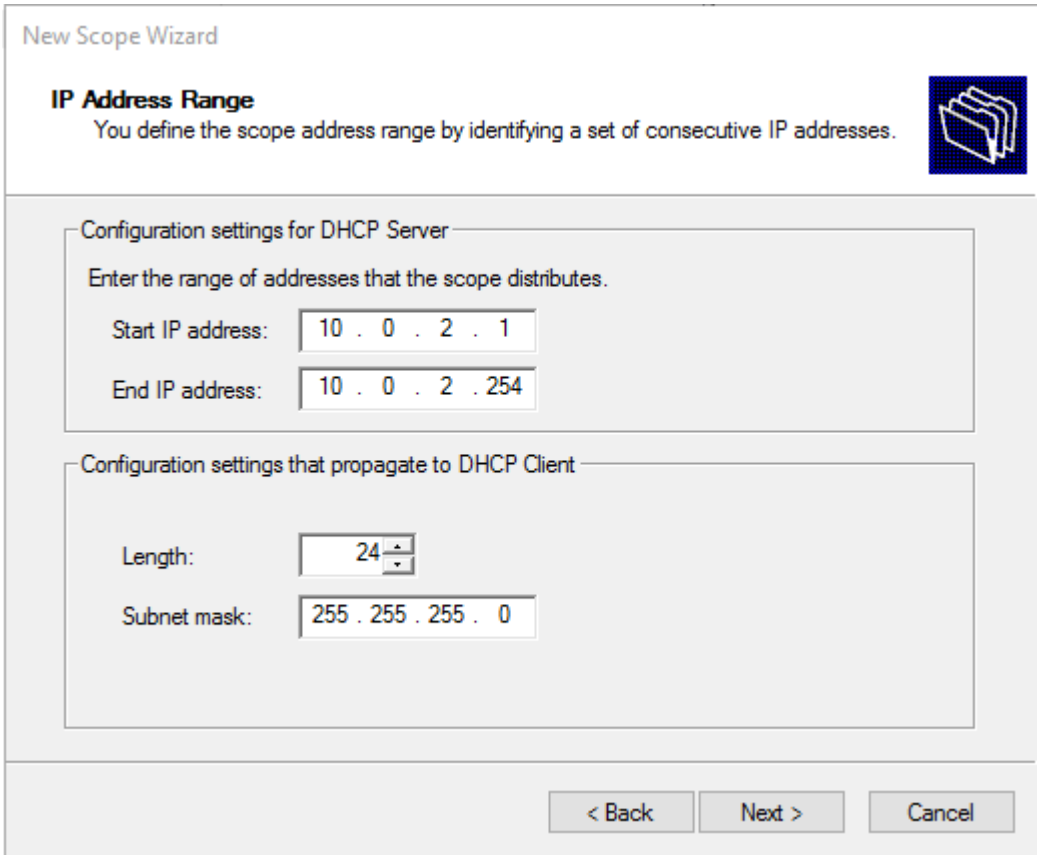
Obrázek 21 Přidání IP adres do pravidla

[Zdroj: vlastní zpracování]

3.3.3 Nastavení DHCP a jeho zabezpečení

Pro nastavení DHCP je nutné určit, pro kolik zařízení bude zhruba sloužit. Jelikož je potřeba si nechat určitou rezervu, zvolil jsem nastavení pro jednu subnetu /24, což je maximálně 253 IP adres s tím, že je jedna adresa rezervována pro router a jedna pro broadcast. Nastavení probíhá v DHCP management okně, kde si prvně vybereme, jestli chceme nastavit DHCP server pro IPv4 adresy nebo IPv6 adresy. Pro tento projekt jsou

vhodné IPv4 adresy. Dále je nutné určit z jakého rozsahu tyto adresy budou. Zvolil jsem adresy z rozsahu 10.0.2.1 – 10.0.2.254 viz. obrázek.



Obrázek 22 Rozsah IP adres z DHCP serveru

[Zdroj: vlastní zpracování]

Jelikož je adresa 10.0.2.255 vyhrazena pro broadcast, musíme nastavit konečný rozsah na 10.0.2.254. Tato adresa se automaticky přiřadí k nastavení DHCP a pokud jsou na ni zaslány data, pošlou se všem zařízením v síti.

Dalším krokem je nastavení výjimek a rezervovaných adres. Pro budoucí využití je dobré rezervovat alespoň 10 IP adres pro případný back up server či další zařízení, které budou potřebovat fixní IP adresu.

Dále je potřeba určit tzv. „lease time“, který určuje, jak dlouho bude IP adresa přiřazena danému zařízení. Je dobré tento čas nastavit na hodnotu, jakou je průměrná doba práce při připojení k této síti. Hodnotu jsem tedy nastavil na 8 hodin.

V posledním kroku je nutné určit default gateway a DNS server. Default gateway je v tomto případě IP adresa routeru a DNS server bude odkazovat sám na sebe.

Zabezpečení DHCP serveru bude probíhat na druhé vrstvě ISO/OSI modelu čili na linkové. Dosaženo toho bude díky konfigurovatelnému switchi s podporou DHCP snoopingu. Switch bude mít nastaven výchozí port DHCP serveru a pokud dostane DHCP offer pakety z jiného portu, automaticky je zahodí. Tím se zamezí potencionálnímu útoku na DHCP server.

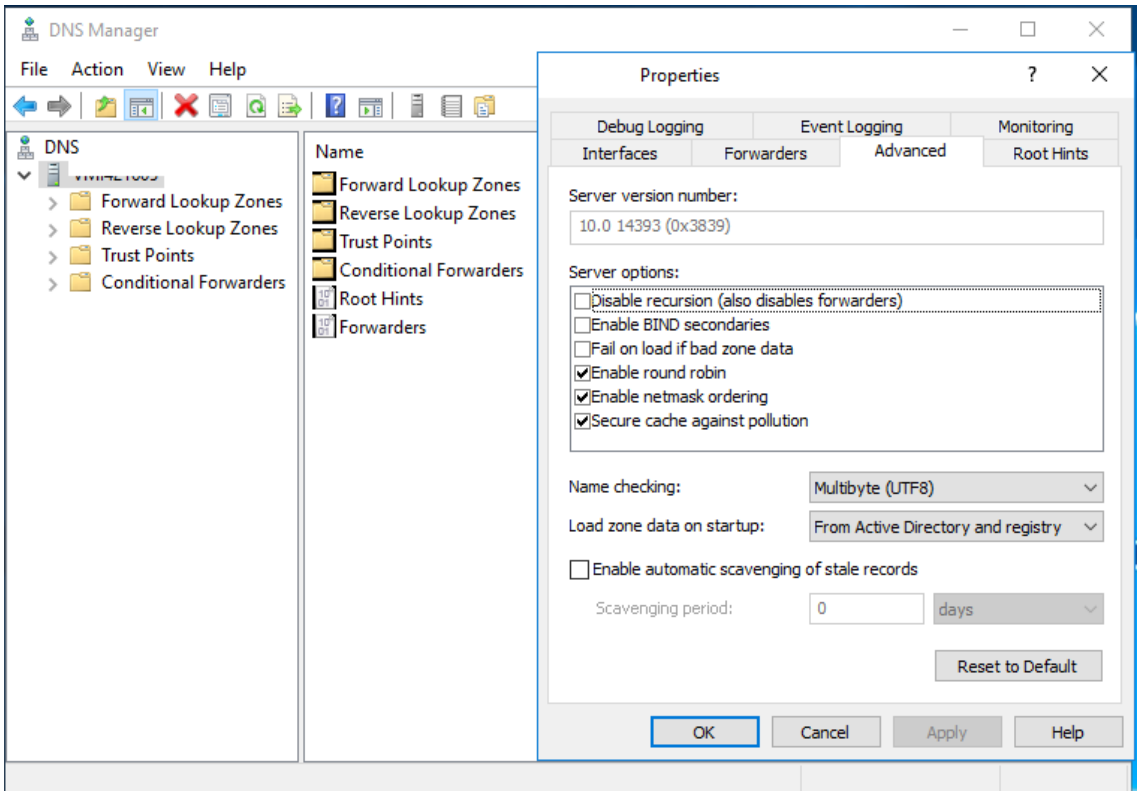
3.3.4 Zabezpečení Remote Desktop Protocolu

Jak bylo zmiňováno, útoky cílené na RDP jsou velmi časté. V době COVID-19 se dokonce takto cílené útoky zvýšili více než o 700%. Zabezpečení RDP na serveru bude tedy spočívat v tom, že bude povolen pouze z privátní sítě a pouze pro určité IP adresy. Samozřejmostí je nutnost připojení ze zařízení, které má síťový level autentizace. Tyto připojení budou také monitorována a vyhodnocována za pomoci členů týmu. Z internetu se místo přes RDP bude dát připojit k serveru pomocí VNC klienta.

3.3.5 Zabezpečení DNS

Jelikož se nezabezpečený DNS server může útočníky využívat pro reflexivní útoku, je třeba tuto službu řádně zabezpečit. Pokud je povolena rekurze v DNS serveru, útočník může podvrhnout zdrojovou IP adresu, na kterou jsou zasílány odpovědi s informacemi o doménovém jménu. Tato adresa je cílem útoku a může dojít k částečnému či úplnému odstavení zařízení s touto IP adresou. Jelikož v tomto projektu rekurze není potřeba, je možné ji vypnout a zamezit tak případným útokům.

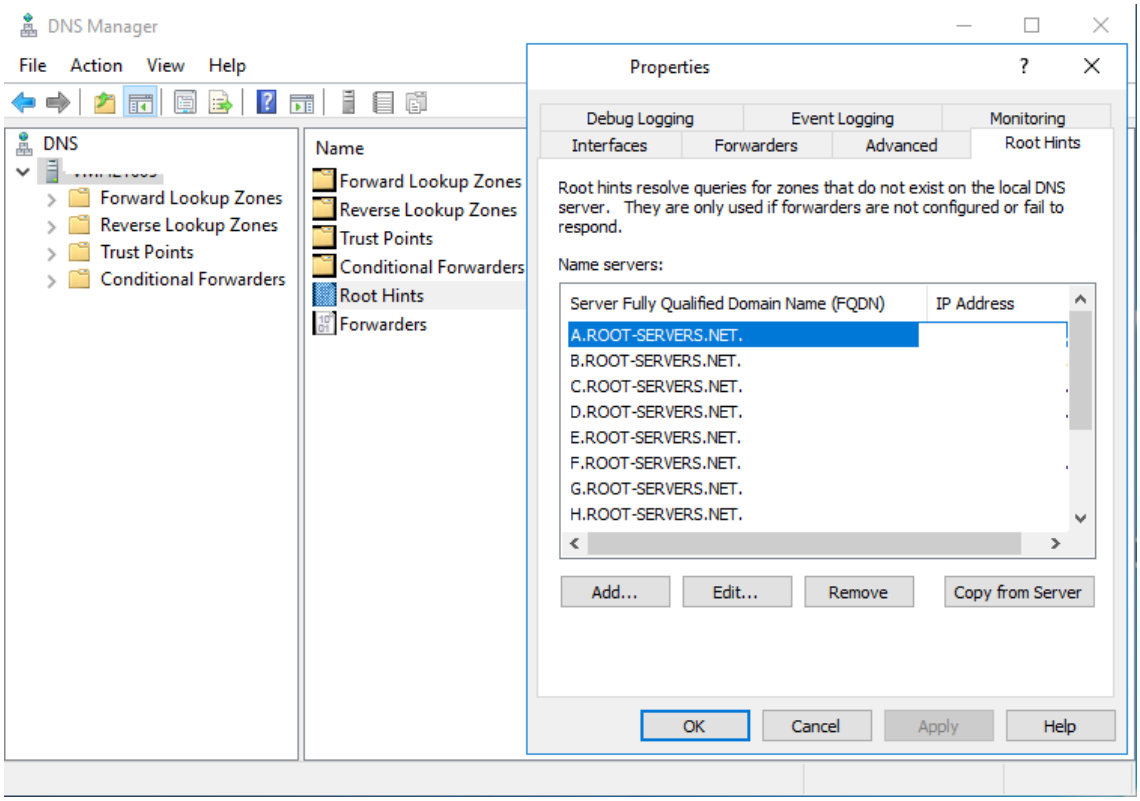
Vypnout se dá z DNS manageru, který je stejně jako DHCP manager v administrative tools. Po spuštění je nutné najet na možnosti DNS serveru a v záložce Advanced zaškrtnout pole „Disable recursion“.



Obrázek 23 Zakázaní rekurze u DNS serveru

[Zdroj: vlastní zpracování]

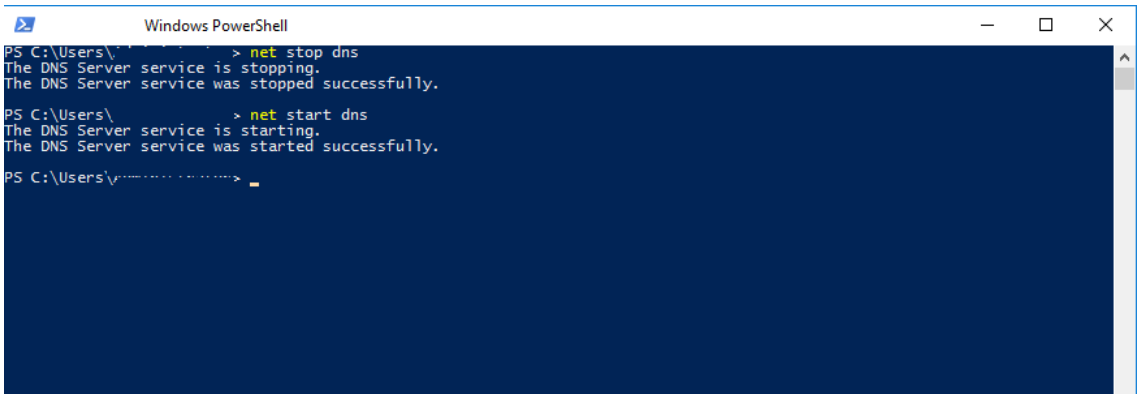
Po zakázání rekurze přepneme do záložky „Root Hints“ a zde je třeba vymazat všechny záznamy.



Obrázek 24 Smazání Root Hints

[Zdroj: vlastní zpracování]

Po smazání všech Root Hints je třeba DNS službu restartovat. To můžeme provést buď restartem celého zařízení, případně přes powershell příkazy „net stop dns“ a „net start dns“ viz. obrázek níže.



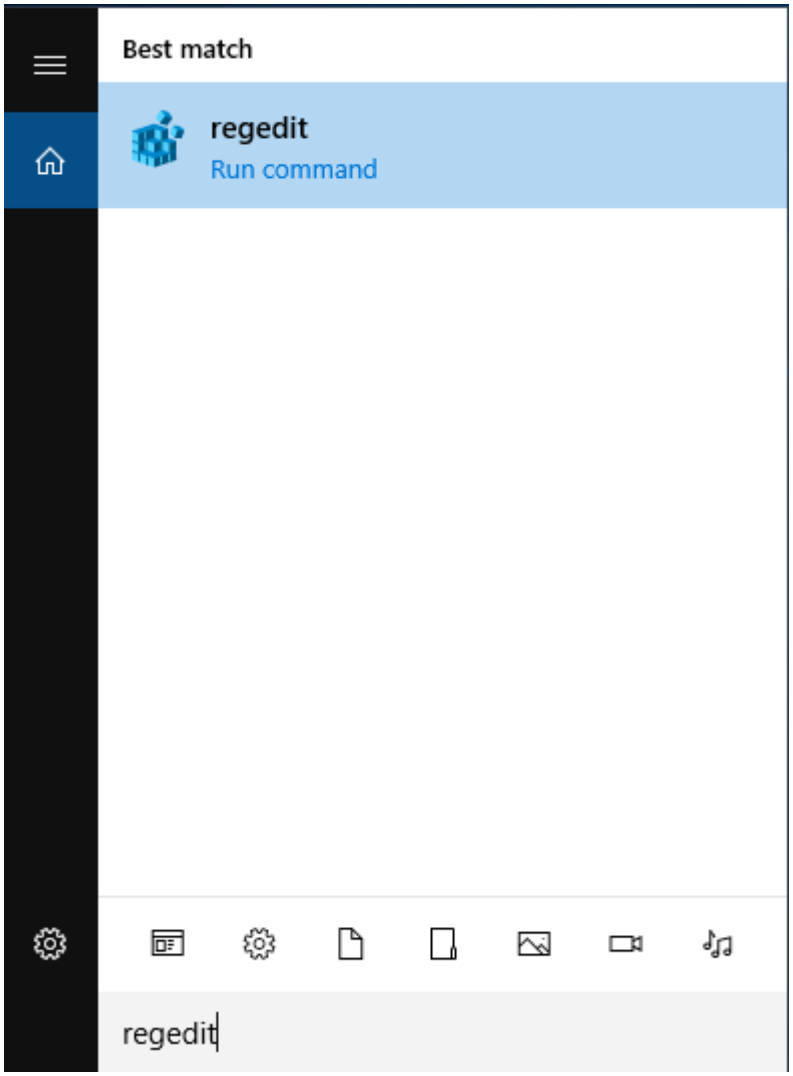
Obrázek 25 Příklad restartování DNS služby

[Zdroj: vlastní zpracování]

3.3.6 Zabezpečení NETBIOS služeb a SMB protokolu

Služby NETBIOSu běží na portech 137, 138 a 139. SMB protokol na novějších systémech poslouchá na portu 445. I když mají služby NETBIOSu dodnes několik bezpečnostní mezer, jsou nainstalovány ve výchozím nastavení systému. Pokud pro služby v projektu není využití, dají se zablokovat. Tato blokace může proběhnout přes blokaci daných portů v rámci firewallu nebo zablokováním služeb v registrech zařízení.

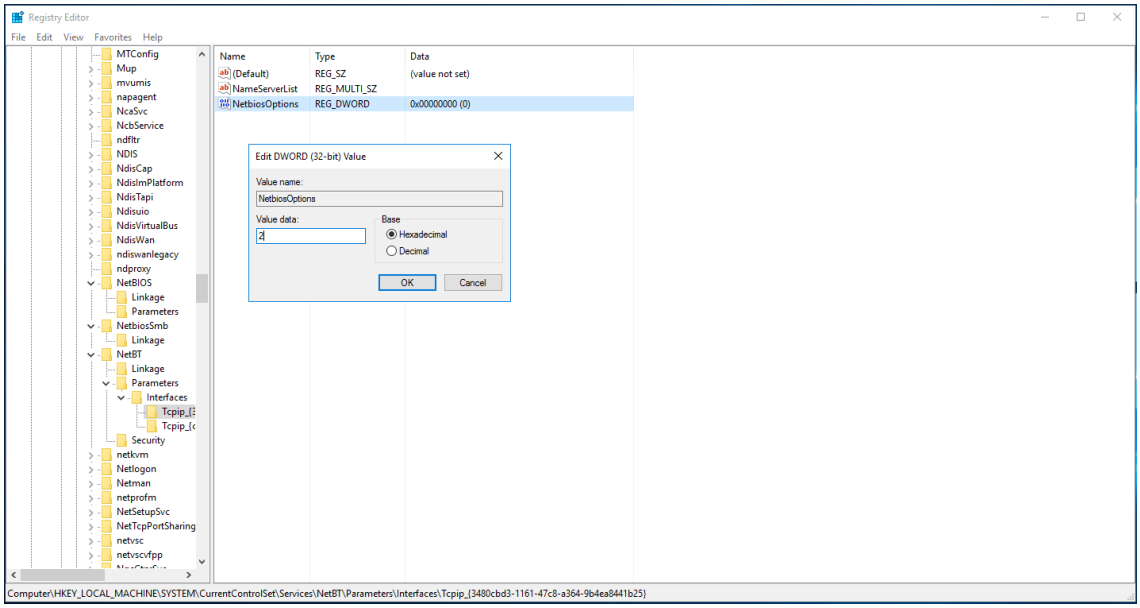
Upravit registry můžeme v editoru registrů. Tam se dostaneme vyhledáním řetězce „regedit“.



Obrázek 26 Vyhledání editoru registrů

[Zdroj: vlastní zpracování]

Registry pro blokaci NETBIOS služby najdeme v HKEY_LOCAL_MACHINE/SYSTÉM/CurrentControlSet/Services/NetBT/Parameters. V této složce najedeme na Interfaces a v každém interface musíme přepsat registr NetbiosOptions na hodnotu 2 podle manuálu Microsoftu. Výchozí nastavení této hodnoty je 0. Pro aplikaci těchto změn je třeba restartovat zařízení.



Obrázek 27 Změna hodnoty registru

[Zdroj: vlastní zpracování]

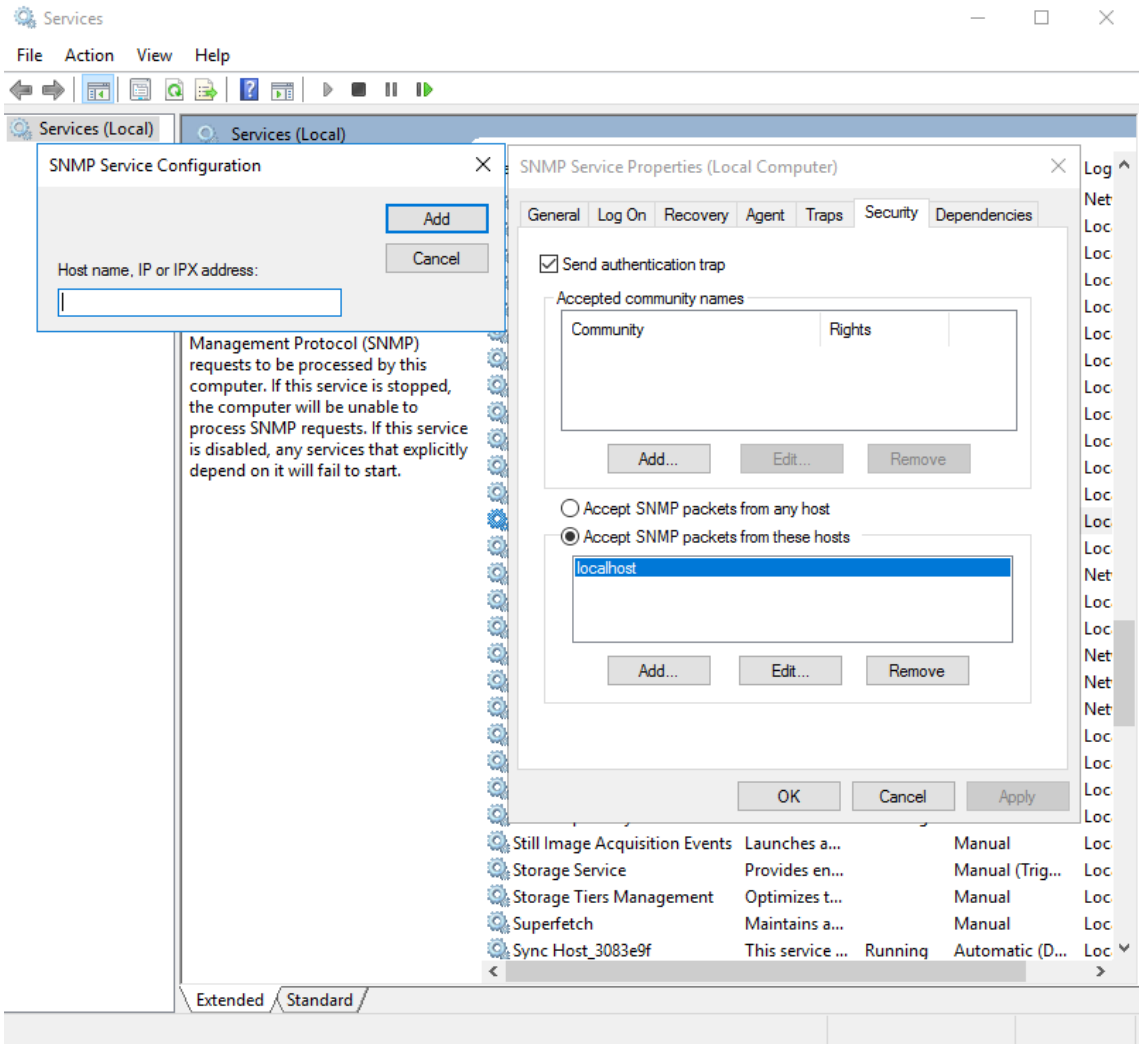
Pokud je třeba mít službu spuštěnou pouze pro některé zařízení, je možné udělit výjimku přes firewallová pravidla.

3.3.7 Zabezpečení SNMP

Pro monitoring stavu zařízení se může využít SNMP protokolu. Příkladem může být monitorování switche, ale i jeho management, který potom probíhá pomocí tzv. MIB souborů.

Monitorovat se dá i samotný server, pokud je SNMP zapnuté, poslouchá na portu 161. Dodnes je to stále běžně využívaný protokol. Má ale bezpečnostní mezery, a proto je vhodné nastavit přijímání SNMP paketů pouze hostům, u kterých je to potřeba.

Ve Windows se konkrétní hosté dají povolit ve službách, které lze najít pod pojmem services.msc. Zde si najdeme službu SNMP service a v záložce Security můžeme přidat hosta, od kterého budou SNMP pakety přijaty.



Obrázek 28 Přidání hosta pro SNMP server

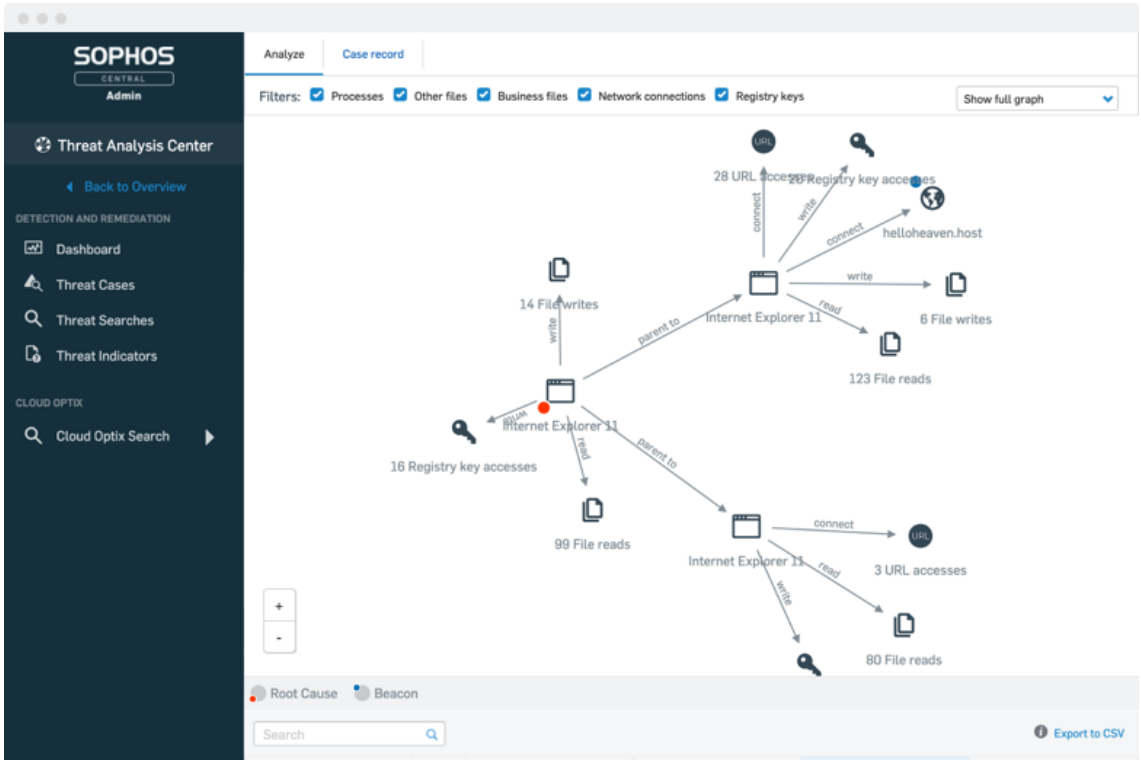
[Zdroj: vlastní zpracování]

3.3.8 Antivirus a threat hunting software

Při bezpečnosti by se nemělo zapomenout na antivirový software, který poskytuje ochranu při kontrole stažených souborů, ale může zastavit útočníky před provedením škodlivého skriptu například v power shellu.

Pokud se útočníci už dostanou do sítě, popřípadě získají kontrolu nad serverem, je dobré mít threat hunting software. Ten slouží k tomu, abychom mohli nalézt přesný vektor útoku a zjistit, co všechno útočníci stihli před odpojením zařízení ze sítě udělat, jaké programy k tomu použili, jestli byl nějaký soubor stažen, popřípadě odkud apod. Některé threat hunting softwary také poskytují podporu remote shellu na nainstalovaných

zařízeních, přes který je možné se zařízením pracovat, aniž bychom museli být fyzicky přítomni u něj.



Obrázek 29 Příklad vectoru - sophos threat hunting software

[Zdroj: 14]

3.3.9 Zálohování a šifrování

V neposlední řadě je potřeba mít nastaveno zálohování dat a jejich šifrování. Zálohování bude zajištěno dvěma disky v serveru připojenými do RAID1. Zálohy se také jednou za den budou ukládat na externí zařízení, které bude odpojené od sítě.

Šifrování bude probíhat nástrojem, který je implementován ve Windows. Tímto nástrojem je BitLocker. Slouží k šifrování dat na celém disku. Tato data jsou šifrována buď heslem nebo vygenerovaným klíčem.

3.4 KONTROLA ZABEZPEČENÍ

Důležité není jen zabezpečit porty a služby, které na nich běží, ale také toto zabezpečení udržovat. Je tedy nezbytné, aby se prováděly testy v pravidelných intervalech, případně

se nasimuloval útok, který může od potencionálního útočníka přijít. Každý člen týmu by měl být zaškolen tak, aby testy uměl provádět.

Nejjednodušším testem je test přes nmap, při znalosti jednoduchého skriptu ho může udělat každý, kdo má připojení k internetu a nainstalovaný tento nástroj. Musí být určeno, který člen bude test provádět a z jaké IP adresy, tato IP adresa se přidá na testovací čas do white listu, aby nebyla monitorovacím testem zablokována.

3.4.1 Interpretace výstupu

Pro určitou formu dokumentace musí být výstup z každého testu nějakým způsobem interpretován. Základní formou interpretace bude výstup ve formě textového souboru, který bude vytvořen přímo nástrojem nmap. Jak jsem již zmiňoval v analytické části, při testu stačí do nástroje přidat argument -o a název, jakým bude soubor pojmenován. Pro lepší přehlednost je nastaven systém názvů na „Test_hlavniho_serveru_YYYY_MM_DD“, podle kterého je jasné, kdy byl test pořízen. Každý člen týmu, který bude tyto testy provádět musí být kompletně srozuměn se zabezpečením serveru, aby mohl rozpoznat situace, kdy bude na serveru zabezpečení v jiném stavu, než by mělo být. Data musí být zašifrována, aby při jejich případném úniku nezískal útočník informace o zranitelnostech serveru.

Také je důležité myslet na to, že nmap vrací stav portu jako open, filtered, closed nebo unfiltered. Pokud je port ve stavu open, znamená to, že server na tomto portu poslouchá a přijímá tedy pakety, které jsou směřované na tento port.

Stav closed znamená, že na serveru neběží žádná služba, která by na daném portu poslouchala. Není však vyloučené, že při instalaci nějaké služby se tento port nepřepne do stavu open.

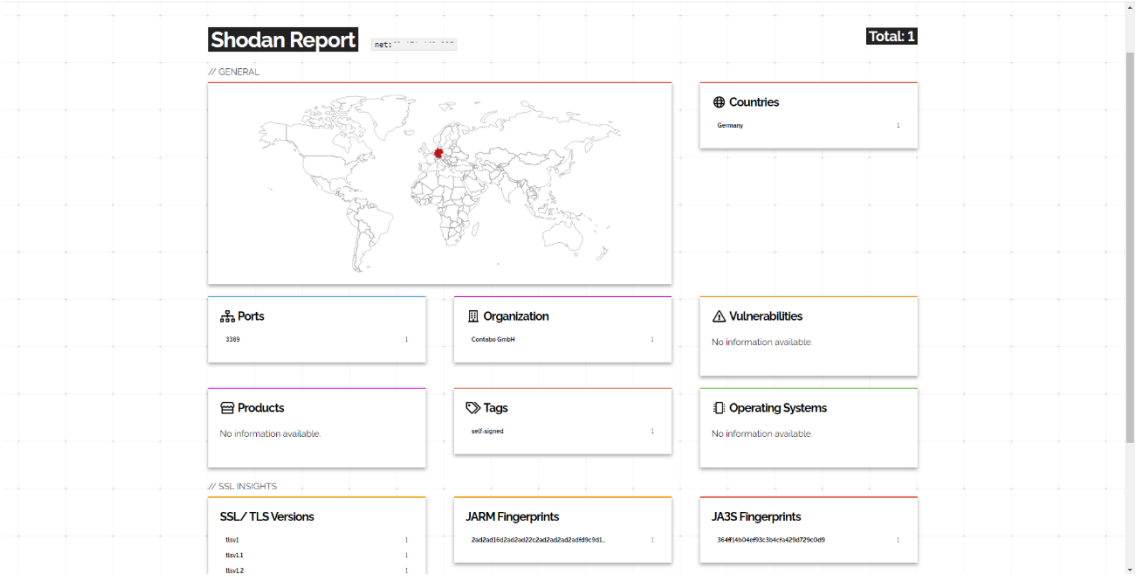
Filtered neboli filtrovaný port znamená to, že před serverem je aktivní firewall nebo jiný typ filtru a nmap nedokáže zjistit, zda je port otevřený nebo zavřený.

Poslední možností je unfiltered. Tato možnost se objeví tehdy, když server nmapu na dotaz odpověděl, ale ten nedokázal zcela jistě určit, o jaký port se jedná. Vrací tedy hodnoty open/filtered nebo closed/filtered a to tehdy, když neví, v jakém stavu se port nachází.

Nejdůležitějšími porty z pohledu bezpečnosti jsou open porty, jelikož si je může ověřit v podstatě kdokoliv.

3.4.2 Monitoring pomocí Shodan.io

Nástroj Shodan.io jsem již popisoval. Jednou z jeho funkcí je také monitoring zvolených IP adres. Funkce je dostupná v rámci poplatku za členství, které je časově neomezené. V reportu z tohoto nástroje jsou informace o otevřených portech, pokud je server hostovaný třetí stranou, uvádí, která společnost jej hostuje, zobrazuje známé zranitelnosti, snaží se získat informace o operačním systému apod. Report z každého provedeného monitoring lze zaslat na email pro uschování a případnou analýzu.



Obrázek 30 Shodan monitoring

[Zdroj: vlastní zpracování]

3.5 EKONOMICKÉ ZHODNOCENÍ

V rámci navržení kompletní realizace je nutné provést ekonomické zhodnocení projektu a odhadnout náklady na provoz. V první řadě popíšu, jaké náklady budou vynaloženy na zřízení celého projektu a poté přičtu náklady na provoz. Všechny částky budou vypsány včetně DPH.

3.5.1 Nacenění serveru a jeho provoz

Primárně je nutné nacenit server, na kterém vše poběží. Nyní vše funguje na virtuální serveru od společnosti Contabo, která poskytuje hosting virtuálních i dedikovaných serverů. Společnost si za měsíc pronájmu virtuálního serveru účtuje 18.98€, což v přepočtu vychází zhruba na 528 Kč. Z toho je 8.99€ za běh VPS a 9.99€ za operační systém Windows 2016 Datacenter Edition. Roční útrata za provoz serveru je tedy zhruba 6 336 Kč.

Pro lepší manipulaci a celkové konfiguraci serveru je ale plánováno server koupit nový a využívat ho na ostatní služby, které s projektem souvisí. Nový server, který by měl parametry jako v HW požadavcích čili čtyřjádrový CPU a 16GB RAM s dvěma HDD po 1 TB paměti by vyšel na 34 090Kč. Náklady na provoz takového serveru jsou zhruba 3200Kč ročně. Další položkou je Windows server licence. Jak jsem psal v SW požadavcích, nejlepším výběrem bude Windows server 2019 standard. Tato licence stojí 20 890Kč s DPH. Na server je také třeba nainstalovat antivirovou ochranu. Zvolil jsem ochranu od společnosti ESET, která stojí 1 490Kč za rok. Co se týče threat hunting softwaru, jeden z poskytovatelů je společnost Sophos, tento software bude stát zhruba 2 500Kč za rok. Poslední položkou je monitorovací systém od společnosti Solar Winds. Platba za tento systém je jednorázová a činí okolo 25 000Kč. Ostatní software pro provoz serveru je dostupný zdarma.

3.5.2 Celkové nacenění projektu

V týmu je 8 členů, kteří práci vykonávají dobrovolně a bez nároku na mzdu. Každý člen má jasně dané úkoly, na které má nastavené pravomoce. Z tohoto důvodu odpadá velká část finančních nákladů a je možné tyto prostředky využít právě pro nákup hardwaru či softwaru.

Každý člen týmu má své zařízení, které využívá k administraci serveru a k řešení problémů na serveru. Tyto zařízení využívají členové i pro osobní účely, tudíž žádné náklady nevznikají.

Počáteční náklady na koupi nového serveru a softwaru jsou zhruba 84 670Kč. Do těchto nákladů je započítána již energie na jeden rok a koupě ročních licencí daných softwarů. Průběžné roční náklady budou po prvním roce 7 190Kč za rok.

Tyto náklady se platí z příspěvků, které jsou zasílány hráči. Pokud je server dostatečně zabezpečen a hráči nepociťují výpadky, či jeho ohrožení, příspěvky jsou vyšší. Pokud by server zabezpečen nebyl, nemotivovalo by to hráče na jeho chod přispívat, a tudíž by se finance vyhrazené na chod serveru mohly krátit a hráči by mohli odcházet na konkurenční servery. Další věcí je časová úspora, která tímto zabezpečením nastane.

ZÁVĚR

Postupy pro analýzu současného zabezpečení jsou detailně popsány a doplněny obrázky, tudíž by ji měl zvládnout i někdo, kdo má alespoň základní znalosti v IT prostředí.

V praktické části byly navrhnuty opatření proti zranitelnostem, které byly zjištěny analýzou a následně byly na server aplikovány. Tato opatření jsou jedním krokem k zabezpečení. Jak jsem zmiňoval, je důležité, aby se analýza prováděla v určitých intervalech, jelikož se může stát, že například aktualizace systému otevře nežádoucí port, který by měl být blokovaný.

Členové týmu byli řádně zaškoleni do problematiky a měli by zvládat analýzu podle popisu provést. Z následné analýzy dokážou udělat report, který je pak uschován pro dokumentaci o projektu.

Z pohledu aktualizací systému a ostatních aplikací byl zvolen jeden člen, který bude udržovat všechny nainstalované programy aktuální a tím se sníží riziko potencionálních zero-day útoků.

Pokud by proběhl úspěšný útok na server, je zde implementován software, pomocí kterého určíme, kudy k průniku došlo a poté lze tuto zranitelnost nějakým způsobem zabezpečit.

Při případném ransom ware útoku budou k dispozici zálohy, které budou uloženy offline pro případ potřeby. Případně se dá použít nástroj „rollback“, který je implementován v threat hunting softwaru. V rámci ošetření případného úniku dat budou všechna data uložená na serveru šifrována.

V poslední části jsem se věnoval ekonomickému zhodnocení celého projektu, který bude stát při migraci na nový server zhruba 84 670,-. Roční investice na provoz serveru jsou potom 7 190,-.

V rámci této diplomové práce jsem měl za úkol navrhnout komplexní a udržitelné zabezpečení herního serveru, což se podařilo. Řešení je navíc navrženo tak, aby měl server určitou rezervu ve výpočetním výkonu pro obsluhu dalších služeb, které jsou

spojené s provozem serveru. Pro tyto účely nebude nutné dělat nějaké větší zásahy a změny mohou být provedeny za běhu serveru.

SEZNAM POUŽITÝCH ZDROJŮ

[1] ONDRÁK, Viktor *Počítačové sítě* [přednáška]. Brno: VUT v Brně, Fakulta podnikatelská, 2018.

[2] HORÁK, Jaroslav *Počítačové sítě pro začínající správce*, Computer press 2011. ISBN: 978-80-251-3176-3

[3] CLARK, Ben *RTFM: Red team field manual*, Ben Clark 2013. ISBN-13: 978-1494295509

[4] HUNT, Craig. TCP/IP network administration. 3rd edition. Sebastopol: O'Reilly & Associates, 1992. ISBN 0-937175-82-X.

[5] DONAHUE, Gary A. *Kompletní průvodce síťového experta*. Vyd. 1. Brno: Computer Press, 2015. 528 s. ISBN 9788025122471.

[6] VAVREČKOVÁ, *Šárka Teoretická informatika* [přednáška]. Opava: Slezská univerzita, Fakulta filozoficko-přírodovědecká, 2017.

[7] KUROSE, James, Keith ROSS a Jindřich JONÁK. Počítačové sítě. 1. vyd. V Brně: Computer Press, 2014, 622 s. : il. portréty, grafy, tab. ISBN 9788025138250

[8] CZ.NIC - O doménách a DNS. CZ.NIC [online]. Copyright © 2020 CZ.NIC, z. s. p. o. [cit. 26.02.2021]. Dostupné z: https://www.nic.cz/page/312/o-domenach-a-dns/

[9] RFC 2251. Lightweight Directory Access Protocol (v3) [online]. M. WahlCritical Angle Inc., T. HowesNetscape, Communications Corp., S. Kille, Isode Limited. December 1997 [cit. 09.03.2021]. Dostupné z: https://www.ietf.org/rfc/rfc2251.txt

[10] Microsoft – Synchronizace protokolu LDAP s Azure Active Directory [online]. Copyright © 2021 Microsoft [cit. 26.02.2021]. Dostupné z: https://docs.microsoft.com/cs-cz/azure/active-directory/fundamentals/sync-ldap

[11] IETF Simple Service Discovery Protocol/1.0 [online]. Yaron Y. Goland, Ting Cai, Paul Leach, Ye Gu, Microsoft Corporation, Shivaun Albright, Hewlett-Packard Company. October 28, 1999. [cit. 09.03.2021]. Dostupné z: https://tools.ietf.org/html/draft-cai-ssdpv1-03

[12] Nmap package description [online]. Copyright © 2019 Offsec Inc. All rights reserved. [cit. 15.03.2021]. Dostupné z: https://tools.kali.org/information-gathering/nmap

[13] SMEJKAL, Vladimír a Karel RAIS. Řízení rizik ve firmách a jiných organizacích. 4., aktualiz. a rozš. vyd. Praha: Grada, 2013. Expert (Grada). ISBN 978-80-247-4644-9.

[14] Sophos Ltd. [online]. © 1997-2021 Sophos Ltd. All rights reserved. [cit. 24.04.2021]. Dostupné z: https://www.sophos.com/en-us.aspx

SEZNAM POUŽITÝCH ZKRATEK A SYMBOLŮ

NAT Network Address Translation

TCP Transmission Control Protocol

UDP User Datagram Protocol

SSH Secure Shell

TCP/IP Transmission Control Protocol/Internet Protocol

CSMA/CD Carrier Sense Multiple Access with Collision Detection

TTL Time To Live

DHCP Dynamic Host Configuration Protocol

NTP Network Time Protocol

LDAP Lightweight Directory Access Protocol

AD Active Directory

SMB Server Message Block

MMORPG Massively Multiplayer Online Role-Playing Game

DDoS Distributed Denial of Service

FTP File Transfer Protocol

SMTP Simple Mail Transfer Protocol

TFTP Trivial File Transfer Protocol

RDP Remote Desktop Protocol

CPU Central Processing Unit

HDD Hard Disk Drive

RAM Random Access Memory

VPS Virtual Private Server

SEZNAM POUŽITÝCH OBRÁZKŮ

SEZNAM POUŽITÝCH TABULEK

SEZNAM POUŽITÝCH GRAFŮ

SEZNAM PŘÍLOH